

As part of NCA duties to help securing the cyberspace and الوطني، تود الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني للمساعدة في حماية الفضاء السيبراني وعنه الفضاء السيبراني للمساعدة في حماية الفضاء السيبراني وعنه المعنوبين المساعدة في حماية الفضاء السيبراني ومعن المساعدة في حماية الفضاء السيبراني ومعن المساعدة في حماية الفضاء المسجلة من قبل protecting national interests, NCA provides the weekly summary of the National الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل published vulnerabilities by the National Institute of Standards and Institute of Standards and Technology (NIST) National Technology (NIST) National Vulnerability Database (NVD) for the للأسبوع من 10 ديسمبر إلى 17 ديسمبر. علماً week from 10th of December to 17th of December. Vulnerabilities Common Vulnerability Scoring System are scored using the Common Vulnerability Scoring System

- (CVSS) standard as per the following severity:
 Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

- عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
 - عالى: النتيجة الأساسية لـCVSS 7.0-8.9
 - متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0
 - منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVS S Score	Severity
	google -				
	chromecast_firmw	Missing Permission checks resulting in unauthorized access and			I
<u>CVE-2023-48417</u>	are	Manipulation in KeyChainActivity Application	2023-12-11	9.8	Critical
	google -	LL Deet shell uulusershilitu essulting in Drivilege seesletign in s			
CVE-2023-48424	chromecast_firmw are	U-Boot shell vulnerability resulting in Privilege escalation in a production device	2023-12-11	9.8	Critical
<u>CVL-2023-48424</u>	google -		2023-12-11	9.0	Critical
	chromecast_firmw				
CVE-2023-48425	are	U-Boot vulnerability resulting in persistent Code Execution	2023-12-11	9.8	Critical
	google -				
	chromecast_firmw	An oversight in BCB handling of reboot reason that allows for			
CVE-2023-6181	are	persistent code execution	2023-12-11	9.8	Critical
		SAP BTP Security Services Integration Library ([Node.js]			
		<pre>@sap/xssec - versions < 3.6.0, allow under certain conditions an</pre>			
		escalation of privileges. On successful exploitation, an			
	N - N /	unauthenticated attacker can obtain arbitrary permissions within			
<u>CVE-2023-49583</u>	sap - \@sap\/xssec	the application.	2023-12-12	9.8	Critical
		SAP BTP Security Services Integration Library ([Java] cloud-			
		security-services-integration-library) - versions below 2.17.0 and			
		versions from 3.0.0 to before 3.3.0, allow under certain conditions an escalation of privileges. On successful exploitation, an			
	sap - multiple	unauthenticated attacker can obtain arbitrary permissions within			
CVE-2023-50422	products	the application.	2023-12-12	9.8	Critical
	p. 00000	SAP BTP Security Services Integration Library ([Python] sap-xssec) -		0.0	0
		versions < 4.1.0, allow under certain conditions an escalation of			
		privileges. On successful exploitation, an unauthenticated attacker			
CVE-2023-50423	sap - sap-xssec	can obtain arbitrary permissions within the application.	2023-12-12	9.8	Critical
		SAP BTP Security Services Integration Library ([Golang]			
		github.com/sap/cloud-security-client-go) - versions < 0.17.0, allow			
		under certain conditions an escalation of privileges. On successful			
01/5 2022 50424	sap - cloud-	exploitation, an unauthenticated attacker can obtain arbitrary	2022 12 12	0.0	Cuitical
CVE-2023-50424	security-client-go	permissions within the application.	2023-12-12	9.8	Critical
		A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). Affected products do not properly validate the			
		certificate of the configured UMC server. This could allow an			
		attacker to intercept credentials that are sent to the UMC server			
	siemens - multiple	as well as to manipulate responses, potentially allowing an			
CVE-2023-48427	products	attacker to escalate privileges.	2023-12-12	9.8	Critical
		Nagios XI before version 5.11.3 was discovered to contain a SQL			
<u>CVE-2023-48084</u>	nagios - nagios_xi	injection vulnerability via the bulk modification tool.	2023-12-14	9.8	Critical
		Nagios XI before version 5.11.3 was discovered to contain a			
		remote code execution (RCE) vulnerability via the component			
<u>CVE-2023-48085</u>	nagios - nagios_xi	command_test.php.	2023-12-14	9.8	Critical
		A deserialization vulnerability existed when decode a malicious			
		package.This issue affects Apache Dubbo: from 3.1.0 through			
CV/E_2022 20224	apache - multiple	3.1.10, from 3.2.0 through 3.2.4.	2022 12 15	0.0	Critical
<u>CVE-2023-29234</u>	products		2023-12-15	9.8	Critical

		Users are recommended to upgrade to the latest version, which fixes the issue.			
		Deserialization of Untrusted Data vulnerability in Apache Dubbo.This issue only affects Apache Dubbo 3.1.5.			
		Users are recommended to upgrade to the latest version, which			
CVE-2023-46279	apache - dubbo	fixes the issue.	2023-12-15	9.8	Critica
		A Command Injection vulnerability exists in NETGEAR WNR2000v4 version 1.0.0.70. When using HTTP for SOAP authentication,			
	netgear -	command execution occurs during the process after successful			
CVE-2023-50089	wnr2000_firmware	authentication.	2023-12-15	9.8	Critica
		SAP GUI for Windows and SAP GUI for Java allow an			
		unauthenticated attacker to access information which would otherwise be restricted and confidential. In addition, this			
		vulnerability allows the unauthenticated attacker to write data to			
	sap - multiple	a database table. By doing so the attacker could increase response			
<u>CVE-2023-49581</u>	products	times of the AS ABAP, leading to mild impact on availability.	2023-12-12	9.4	Critica
		The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, macOS Sonoma 14.2, watchOS 10.2,			
	apple - multiple	iOS 17.2 and iPadOS 17.2, tvOS 17.2. Processing web content may			
<u>CVE-2023-42890</u>	products	lead to arbitrary code execution.	2023-12-12	8.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
CVE-2023-42910	apple - macos	Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2023-12-12	8.8	High
<u> </u>		A vulnerability has been identified in Opcenter Quality (All	202J 12-12	0.0	i ngi i
		versions), SIMATIC PCS neo (All versions < V4.1), SINUMERIK			
		Integrate RunMyHMI /Automotive (All versions), Totally Integrated			
		Automation Portal (TIA Portal) V14 (All versions), Totally Integrated Automation Portal (TIA Portal) V15.1 (All versions),			
		Totally Integrated Automation Portal (TIA Portal) V15.1 (All Versions),			
		versions), Totally Integrated Automation Portal (TIA Portal) V17			
		(All versions), Totally Integrated Automation Portal (TIA Portal)			
		V18 (All versions < V18 Update 3). When accessing the UMC Web-			
	siemens - multiple	UI from affected products, UMC uses an overly permissive CORS policy. This could allow an attacker to trick a legitimate user to			
CVE-2023-46281	products	trigger unwanted behavior.	2023-12-12	8.8	High
	microsoft - multiple	Internet Connection Sharing (ICS) Remote Code Execution			
CVE-2023-35630	products	Vulnerability	2023-12-12	8.8	High
CVE-2023-35634	microsoft - multiple products	Windows Bluetooth Driver Remote Code Execution Vulnerability	2023-12-12	8.8	High
<u>CVL-2023-33034</u>	microsoft - multiple	Windows Blactooth Driver Remote Code Execution Vallerability	2023-12-12	0.0	Ingii
<u>CVE-2023-35639</u>	products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2023-12-12	8.8	High
	microsoft - multiple	Internet Connection Sharing (ICS) Remote Code Execution			
<u>CVE-2023-35641</u>	products	Vulnerability	2023-12-12	8.8	High
CVE-2023-36006	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-12-12	8.8	High
	products	A cross-site request forgery (CSRF) in Fortinet FortiVoiceEnterprise		0.0	
		version 6.4.x, 6.0.x, FortiSwitch version 7.0.0 through 7.0.4, 6.4.0			
		through 6.4.10, 6.2.0 through 6.2.7, 6.0.x, FortiMail version 7.0.0			
		through 7.0.3, 6.4.0 through 6.4.6, 6.2.x, 6.0.x FortiRecorder			
		version 6.4.0 through 6.4.2, 6.0.x, 2.7.x, 2.6.x, FortiNDR version 1.x.x allows a remote unauthenticated attacker to execute			
	fortinet - multiple	commands on the CLI via tricking an authenticated administrator			
CVE-2022-27488	products	to execute malicious GET requests.	2023-12-13	8.8	High
		A use of externally-controlled format string in Fortinet FortiProxy			
		versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, FortiOS versions 7.4.0, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through			
		6.4.12, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiPAM			
		versions 1.0.0 through 1.0.3 allows attacker to execute			
	fortinet - multiple	unauthorized code or commands via specially crafted API			
CVE-2023-36639	products	requests. A double free in Fortinet FortiOS versions 7.0.0 through 7.0.5,	2023-12-13	8.8	High
		FortiPAM version 1.0.0 through 1.0.3, 1.1.0 through 1.1.1 allows			
	fortinet - multiple	attacker to execute unauthorized code or commands via			
CVE-2023-41678	products	specifically crafted request.	2023-12-13	8.8	High
		A improper neutralization of special elements used in an os			
		command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 allows attacker to execute unauthorized code			
CVE-2023-48782	fortinet - fortiwlm	or commands via specifically crafted http get request parameters	2023-12-13	8.8	High
<u> 2020 +0/02</u>		An improper neutralization of special elements used in a command	12 13	5.0	
		('Command Injection') vulnerability [CWE-77] in FortiPortal version			
		7.2.0, version 7.0.6 and below may allow a remote authenticated			
	fortingt multiple	attacker with at least R/W permission to execute unauthorized			
CVE-2023-48791	fortinet - multiple products	commands via specifically crafted arguments in the Schedule System Backup page field.	2023-12-13	8.8	High
<u> </u>	products	** UNSUPPORTED WHEN ASSIGNED **A improper limitation of a	202J 12-1J	0.0	i ligit
	fortinet - multiple	pathname to a restricted directory ('path traversal') vulnerability			
		[CWE-22] in Fortinet FortiWAN version 5.2.0 through 5.2.1 and			

		version 5.1.1. through 5.1.2 may allow an authenticated attacker			
		to read and delete arbitrary file of the system via crafted HTTP or HTTPs requests.			
		** UNSUPPORTED WHEN ASSIGNED **An improper authentication			
		vulnerability [CWE-287] in Fortinet FortiWAN version 5.2.0			
		through 5.2.1 and version 5.1.1 through 5.1.2 may allow an			
CVE-2023-44252	fortinet - multiple products	authenticated attacker to escalate his privileges via HTTP or HTTPs requests with crafted JWT token values.	2023-12-13	8.8	High
	products	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus	2023 12 13	0.0	
		Platform Plugin 3.18.0-03 and earlier allows attackers to send an			
	jenkins -	HTTP request to an attacker-specified URL and parse the response			
<u>CVE-2023-50766</u>	nexus_platform	as XML. A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus	2023-12-13	8.8	High
		Platform Plugin 3.18.0-03 and earlier allows attackers to connect			
		to an attacker-specified HTTP server using attacker-specified			
	jenkins -	credentials IDs obtained through another method, capturing			
CVE-2023-50768	nexus_platform	credentials stored in Jenkins.	2023-12-13	8.8	High
		A cross-site request forgery (CSRF) vulnerability in Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier allows attackers to			
	jenkins -	connect to an attacker-specified URL using an attacker-specified			
CVE-2023-50778	paaslane_estimate	token.	2023-12-13	8.8	High
		Path traversal in Zoom Desktop Client for Windows, Zoom VDI			
		Client for Windows, and Zoom SDKs for Windows may allow an			
CVE-2023-43586	zoom - multiple products	authenticated user to conduct an escalation of privilege via network access.	2023-12-13	8.8	High
<u></u>	p. 044005	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3	12	0.0	1 1811
		through 1.1.9.3 could allow an attacker to execute remote code.			
		Due to improper authority checks the attacker could perform			
CVE 2022 4E19E	ibm - multiple	operations on the PC under the user's authority. IBM X-Force ID: 268273.	2022 12 14	8.8	⊔iab
<u>CVE-2023-45185</u>	products	Type confusion in V8 in Google Chrome prior to 120.0.6099.109	2023-12-14	0.0	High
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-6702	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
		Use after free in Blink in Google Chrome prior to 120.0.6099.109			
		allowed a remote attacker to potentially exploit heap corruption	2022 12 14		L li ala
<u>CVE-2023-6703</u>	google - chrome	via a crafted HTML page. (Chromium security severity: High) Use after free in libavif in Google Chrome prior to 120.0.6099.109	2023-12-14	8.8	High
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-6704	google - chrome	via a crafted image file. (Chromium security severity: High)	2023-12-14	8.8	High
		Use after free in WebRTC in Google Chrome prior to			
		120.0.6099.109 allowed a remote attacker to potentially exploit			
CVE-2023-6705	google - chrome	heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
	8008.0 0	Use after free in FedCM in Google Chrome prior to 120.0.6099.109			
		allowed a remote attacker who convinced a user to engage in			
		specific UI interaction to potentially exploit heap corruption via a	2022 42 44		1.1.1.
<u>CVE-2023-6706</u>	google - chrome	crafted HTML page. (Chromium security severity: High) Use after free in CSS in Google Chrome prior to 120.0.6099.109	2023-12-14	8.8	High
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-6707	google - chrome	via a crafted HTML page. (Chromium security severity: Medium)	2023-12-14	8.8	High
		A vulnerability has been identified in SINEC INS (All versions < V1.0			
		SP2 Update 2). Affected software does not correctly validate the			
		response received by an UMC server. An attacker can use this to crash the affected software by providing and configuring a			
	siemens - multiple	malicious UMC server or by manipulating the traffic from a			
<u>CVE-2023-48431</u>	products	legitimate UMC server (i.e. leveraging CVE-2023-48427).	2023-12-12	8.6	High
		In SAP Commerce Cloud - versions HY_COM 1905, HY_COM 2005,			
		HY_COM2105, HY_COM 2011, HY_COM 2205, COM_CLOUD 2211,			
		a locked B2B user can misuse the forgotten password functionality			
	sap -	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable			
<u>CVE-2023-42481</u>	commerce_cloud	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront,	2023-12-12	8.1	High
	commerce_cloud microsoft - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity.			-
	commerce_cloud microsoft - multiple products	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable	2023-12-12 2023-12-12	8.1	-
CVE-2023-35628	commerce_cloud microsoft - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity.			High
CVE-2023-35628	commerce_cloud microsoft - multiple products microsoft - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not	2023-12-12	8.1	High
CVE-2023-35628	commerce_cloud microsoft - multiple products microsoft - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing	2023-12-12	8.1	High
CVE-2023-35628 CVE-2023-36005	commerce_cloud microsoft - multiple products microsoft - multiple products	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary	2023-12-12 2023-12-12	8.1	High High
CVE-2023-35628 CVE-2023-36005	commerce_cloud microsoft - multiple products microsoft - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary files on the Jenkins controller file system.	2023-12-12	8.1	High High
<u>CVE-2023-35628</u> <u>CVE-2023-36005</u>	commerce_cloud microsoft - multiple products microsoft - multiple products	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary	2023-12-12 2023-12-12	8.1	High High
<u>CVE-2023-42481</u> <u>CVE-2023-35628</u> <u>CVE-2023-36005</u> <u>CVE-2023-50764</u> <u>CVE-2023-50774</u>	commerce_cloud microsoft - multiple products microsoft - multiple products jenkins - scriptler	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary files on the Jenkins controller file system. A cross-site request forgery (CSRF) vulnerability in Jenkins	2023-12-12 2023-12-12	8.1	High High High
<u>CVE-2023-35628</u> <u>CVE-2023-36005</u> <u>CVE-2023-50764</u>	commerce_cloud microsoft - multiple products microsoft - multiple products jenkins - scriptler jenkins - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary files on the Jenkins controller file system. A cross-site request forgery (CSRF) vulnerability in Jenkins HTMLResource Plugin 1.02 and earlier allows attackers to delete arbitrary files on the Jenkins controller file system. The issue was addressed with improved memory handling. This	2023-12-12 2023-12-12 2023-12-13	8.1 8.1 8.1	High High High High
CVE-2023-35628 CVE-2023-36005 CVE-2023-50764	commerce_cloud microsoft - multiple products microsoft - multiple products jenkins - scriptler jenkins - multiple	a locked B2B user can misuse the forgotten password functionality to un-block his user account again and re-gain access if SAP Commerce Cloud - Composable Storefront is used as storefront, due to weak access controls in place. This leads to a considerable impact on confidentiality and integrity. Windows MSHTML Platform Remote Code Execution Vulnerability Windows Telephony Server Elevation of Privilege Vulnerability Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary files on the Jenkins controller file system. A cross-site request forgery (CSRF) vulnerability in Jenkins HTMLResource Plugin 1.02 and earlier allows attackers to delete arbitrary files on the Jenkins controller file system.	2023-12-12 2023-12-12 2023-12-13	8.1 8.1 8.1	High High High

		The issue was addressed with improved memory handling. This			
01/5 2022 42002		issue is fixed in macOS Sonoma 14.2. Processing an image may		7.0	112.1
CVE-2023-42882	apple - macos	lead to arbitrary code execution.	2023-12-12	7.8	High
		An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.2, macOS			
	apple - multiple	Ventura 13.6.3, macOS Monterey 12.7.2. A user may be able to			
CVE-2023-42886	products	cause unexpected app termination or arbitrary code execution.	2023-12-12	7.8	High
		The issue was addressed with improved memory handling. This			
		issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2,			
		watchOS 10.2, macOS Ventura 13.6.3, tvOS 17.2, iOS 16.7.3 and			
	apple - multiple	iPadOS 16.7.3, macOS Monterey 12.7.2. Processing an image may			
CVE-2023-42899	products	lead to arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
CVE 2022 42001	annia masas	Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2023-12-12	7.8	⊔iah
<u>CVE-2023-42901</u>	apple - macos	Multiple memory corruption issues were addressed with improved	2023-12-12	7.0	High
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42902	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
<u>CVE-2023-42903</u>	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42904	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app	2022 42 42	7.0	
CVE-2023-42905	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42906	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
<u>CVL 2023 +2300</u>		Multiple memory corruption issues were addressed with improved	2023 12 12	7.0	11181
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
<u>CVE-2023-42907</u>	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42908	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			
		input validation. This issue is fixed in macOS Sonoma 14.2.			
CVE 2022 42000		Processing a maliciously crafted file may lead to unexpected app	2022 12 12	7.0	11:~h
CVE-2023-42909	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42911	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
<u>CVL 2020 (2011</u>		Multiple memory corruption issues were addressed with improved	2023 12 12	7.0	1.1.9.
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42912	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
		Multiple memory corruption issues were addressed with improved			-
		input validation. This issue is fixed in macOS Sonoma 14.2.			
		Processing a maliciously crafted file may lead to unexpected app			
CVE-2023-42926	apple - macos	termination or arbitrary code execution.	2023-12-12	7.8	High
	microsoft - multiple				
CVE-2023-21740	products	Windows Media Remote Code Execution Vulnerability	2023-12-12	7.8	High
	microsoft - multiple				
CVE-2023-35631	products	Win32k Elevation of Privilege Vulnerability	2023-12-12	7.8	High
	microsoft - multiple	Windows Ancillary Function Driver for WinSock Elevation of		7.0	
CVE-2023-35632	products	Privilege Vulnerability	2023-12-12	7.8	High
	microsoft - multiple	Windows Kernel Elevation of Privilege Vulnerability	2022 12 12	70	Lliak
CVE-2023-35633	products	windows kernel Elevation of Privilege vulnerability	2023-12-12	7.8	High
CVE-2023-35644	microsoft - multiple products	Windows Sysmain Service Flowation of Privilego	2023-12-12	7.8	High
<u>CVE-2025-55044</u>	· · · ·	Windows Sysmain Service Elevation of Privilege	2025-12-12	7.0	піві
CVE-2023-36011	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVL-2023-30011	microsoft -	Local Security Authority Subsystem Service Elevation of Privilege	2023-12-12	7.0	LIRI
CVE-2023-36391	windows_11_23h2	Vulnerability	2023-12-12	7.8	High
	microsoft - multiple	Windows Cloud Files Mini Filter Driver Elevation of Privilege	12 12		. н <u>ө</u> г
<u>CVL 2023 30331</u>		C C	2022 12 12	7.8	High
	products	l Vulnerability	2023-17-17	1.0	
<u>CVE-2023-36696</u>	products	Vulnerability A template injection flaw was found in Ansible where a user's	2023-12-12	7.0	8.
	products redhat - multiple	A template injection flaw was found in Ansible where a user's controller internal templating operations may remove the unsafe	2023-12-12	7.0	

		to use a specially crafted file to introduce code injection when supplying templating data.			
		An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 2.3.0 through 7.2.3 may allow an authenticated			
CVE 2022 40716	fortinet - multiple	attacker to execute unauthorized commands via specifically	2023-12-13	7.8	High
CVE-2023-40716	products	crafted arguments when running execute restore/backup . A flaw was found in xorg-server. Querying or changing XKB button	2023-12-13	7.8	High
	us alle st	actions such as moving from a touchpad to a mouse can result in			
	redhat - enterprise_linux_e	out-of-bounds memory reads and writes. This may allow local privilege escalation or possible remote code execution in cases			
CVE-2023-6377	us	where X11 forwarding is involved.	2023-12-13	7.8	High
		The vmwgfx driver contains a local privilege escalation vulnerability that allows unprivileged users to gain access to files			
	vmware - multiple	opened by other processes on the system through a dangling 'file'			
<u>CVE-2022-22942</u>	products	pointer. Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier)	2023-12-13	7.8	High
		are affected by an out-of-bounds write vulnerability that could			
	adaha multinla	result in arbitrary code execution in the context of the current			
CVE-2023-47063	adobe - multiple products	user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
		Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier)			
		are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an			
		allocated memory structure. An attacker could leverage this			
	adobe - multiple	vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim			
CVE-2023-47074	products	must open a malicious file.	2023-12-13	7.8	High
		Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier)			
		are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.			
	adobe - multiple	Exploitation of this issue requires user interaction in that a victim			
<u>CVE-2023-47075</u>	products	must open a malicious file. Adobe Substance 3D Sampler versions 4.2.1 and earlier are	2023-12-13	7.8	High
		affected by an out-of-bounds write vulnerability that could result			
	adobe -	in arbitrary code execution in the context of the current user.			
CVE-2023-48625	substance_3d_sam pler	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
		Adobe Substance 3D Sampler versions 4.2.1 and earlier are			
	adobe -	affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.			
	substance_3d_sam	Exploitation of this issue requires user interaction in that a victim			
<u>CVE-2023-48626</u>	pler	must open a malicious file. Adobe Substance 3D Sampler versions 4.2.1 and earlier are	2023-12-13	7.8	High
		affected by an out-of-bounds write vulnerability that could result			
	adobe -	in arbitrary code execution in the context of the current user.			
CVE-2023-48627	substance_3d_sam pler	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
		Adobe Substance 3D Sampler versions 4.2.1 and earlier are			
	adobe -	affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.			
	substance_3d_sam	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-48628	pler	must open a malicious file.	2023-12-13	7.8	High
		Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result			
	adobe -	in arbitrary code execution in the context of the current user.			
CVE-2023-48629	substance_3d_sam pler	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
		Adobe Substance 3D Sampler versions 4.2.1 and earlier are			0
	adobe -	affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.			
	substance_3d_sam	Exploitation of this issue requires user interaction in that a victim			
<u>VE-2023-48630</u>	pler	must open a malicious file.	2023-12-13	7.8	High
		Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an out-of-bounds write vulnerability that			
		could result in arbitrary code execution in the context of the			
CVE-2023-48632	adobe - multiple products	current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
<u> 2023-40032</u>	ρισααείο	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and	7072-17-12	<i></i>	i ligil
		earlier) are affected by a Use After Free vulnerability that could			
	adobe - multiple	result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			
1	products	victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48633					
<u>CVE-2023-48633</u>		Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an Improper Input Validation vulnerability			
CVE-2023-48633		Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the			

	1				
		Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out of bounds write			
	adobe -	13.1.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the			
	substance 3d desi	context of the current user. Exploitation of this issue requires user			
CVE-2023-48639	gner	interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
		IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local			0
	ibm - multiple	user to exploit a vulnerability in the piodmgrsu command to obtain			
CVE-2023-45166	products	elevated privileges. IBM X-Force ID: 267964.	2023-12-13	7.8	High
		IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local			
	ibm - multiple	user to exploit a vulnerability in the piobe command to escalate			
<u>CVE-2023-45170</u>	products	privileges or cause a denial of service. IBM X-Force ID: 267968.	2023-12-13	7.8	High
	ibm - multiple	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a privileged local user to exploit a vulnerability in the qdaemon command to escalate			
CVE-2023-45174	products	privileges or cause a denial of service. IBM X-Force ID: 267972.	2023-12-13	7.8	High
<u>CVL 2023 43174</u>	products	A vulnerability exists on all versions of Ivanti Connect Secure	2023 12 13	7.0	111811
		below 22.6R2 where an attacker with a foothold on an Ivanti			
		Connect Secure (ICS) appliance can escalate their privileges by			
		exploiting a vulnerable installed application. This vulnerability			
	ivanti - multiple	allows the attacker to gain elevated execution privileges on the			
CVE-2023-41720	products	affected system.	2023-12-14	7.8	High
		SAP Business Objects Business Intelligence Platform is vulnerable			
	can multiple	to stored XSS allowing an attacker to upload agnostic documents in the system which when opened by any other user could lead to			
CVE-2023-42478	sap - multiple products	high impact on integrity of the application.	2023-12-12	7.6	High
<u> </u>	products	A Huawei data communication product has a command injection	2023 12 12	7.0	1.1911
	huawei -	vulnerability. Successful exploitation of this vulnerability may allow			
<u>CVE-2022-48616</u>	ar617vw_firmware	attackers to gain higher privileges.	2023-12-12	7.5	High
		A vulnerability has been identified in SIMATIC PC-Station Plus (All			
		versions), SIMATIC S7-400 CPU 412-2 PN V7 (All versions), SIMATIC			
		S7-400 CPU 414-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU			
		414F-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 416-3 PN/DP			
		V7 (All versions), SIMATIC S7-400 CPU 416F-3 PN/DP V7 (All			
		versions), SINAMICS S120 (incl. SIPLUS variants) (All versions < V5.2 SP3 HF15), SIPLUS S7-400 CPU 414-3 PN/DP V7 (All versions),			
		SIPLUS S7-400 CPU 416-3 PN/DP V7 (All versions). The affected			
		products do not handle HTTP(S) requests to the web server			
		correctly.			
		concerty.			
	siemens - 6es7412-				
	2ek07-	This could allow an attacker to exhaust system resources and			
CVE-2022-47374	0ab0_firmware	create a denial of service condition for the device.	2023-12-12	7.5	High
		A vulnerability has been identified in SIMATIC PC-Station Plus (All			
		versions), SIMATIC S7-400 CPU 412-2 PN V7 (All versions), SIMATIC			
		S7-400 CPU 414-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 414F-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 416-3 PN/DP			
		V7 (All versions), SIMATIC S7-400 CPU 416F-3 PN/DP V7 (All			
		versions), SINAMICS S120 (incl. SIPLUS variants) (All versions <			
		V5.2 SP3 HF15), SIPLUS S7-400 CPU 414-3 PN/DP V7 (All versions),			
		SIPLUS S7-400 CPU 416-3 PN/DP V7 (All versions). The affected			
		products do not handle long file names correctly.			
	siemens - 6es7412-				
CVF-2022-47375	2ek07-	This could allow an attacker to create a buffer overflow and create			
CVE-2022-47375		a denial of service condition for the device.	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl.	2023-12-12	7.5	High
CVE-2022-47375	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS	2023-12-12	7.5	High
CVE-2022-47375	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS	2023-12-12	7.5	High
CVE-2022-47375	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions),	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07- Oab0_firmware	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used.	2023-12-12	7.5	High
<u>CVE-2022-47375</u>	2ek07- 0ab0_firmware siemens - 6gk7243-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to	2023-12-12	7.5	High
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the			
	2ek07- 0ab0_firmware siemens - 6gk7243-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.	2023-12-12	7.5	High
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product. Affected devices improperly handle specially crafted packets sent			
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30-	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.			
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30- 0xe0_firmware	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product. Affected devices improperly handle specially crafted packets sent to port 102/tcp.			
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30- 0xe0_firmware siemens -	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product. Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a denial of service condition.			
<u>CVE-2022-47375</u>	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30- 0xe0_firmware siemens - simatic_drive_contr	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product. Affected devices improperly handle specially crafted packets sent to port 102/tcp.			
	2ek07- 0ab0_firmware siemens - 6gk7243- 8rx30- 0xe0_firmware siemens -	a denial of service condition for the device. A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions), SIMATIC CP 1243-7 LTE (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543-1 (All versions), SINAMICS S210 (6SL5) (All versions >= V6.1 < V6.1 HF2), SIPLUS NET CP 1543-1 (All versions). The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product. Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a denial of service condition.			

	•				
		A vulnerability has been identified in Opcenter Quality (All			
		versions), SIMATIC PCS neo (All versions < V4.1), SINUMERIK			
		Integrate RunMyHMI /Automotive (All versions), Totally Integrated Automation Portal (TIA Portal) V14 (All versions), Totally			
		Integrated Automation Portal (TIA Portal) V14 (All Versions), Totally			
		Totally Integrated Automation Portal (TIA Portal) V16 (All			
		versions), Totally Integrated Automation Portal (TIA Portal) V17			
		(All versions), Totally Integrated Automation Portal (TIA Portal)			
		V18 (All versions < V18 Update 3). The affected application			
		contains an out of bounds write past the end of an allocated buffer			
	ciomono multinlo	when handling specific requests on port 4002/tcp. This could allow			
CVE-2023-46283	siemens - multiple products	an attacker to crash the application. The corresponding service is auto-restarted after the crash.	2023-12-12	7.5	High
072 2023 10203	products	A vulnerability has been identified in Opcenter Quality (All	2023 12 12	7.5	1.1011
		versions), SIMATIC PCS neo (All versions < V4.1), SINUMERIK			
		Integrate RunMyHMI /Automotive (All versions), Totally Integrated			
		Automation Portal (TIA Portal) V14 (All versions), Totally			
		Integrated Automation Portal (TIA Portal) V15.1 (All versions),			
		Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17			
		(All versions), Totally Integrated Automation Portal (TIA Portal) V17			
		V18 (All versions < V18 Update 3). The affected application			
		contains an out of bounds write past the end of an allocated buffer			
		when handling specific requests on port 4002/tcp and 4004/tcp.			
	siemens - multiple	This could allow an attacker to crash the application. The			
<u>CVE-2023-46284</u>	products	corresponding service is auto-restarted after the crash.	2023-12-12	7.5	High
		A vulnerability has been identified in Opcenter Quality (All			
		versions), SIMATIC PCS neo (All versions < V4.1), SINUMERIK Integrate RunMyHMI /Automotive (All versions), Totally Integrated			
		Automation Portal (TIA Portal) V14 (All versions), Totally Integrated			
		Integrated Automation Portal (TIA Portal) V14 (All Versions), Totally			
		Totally Integrated Automation Portal (TIA Portal) V16 (All			
		versions), Totally Integrated Automation Portal (TIA Portal) V17			
		(All versions), Totally Integrated Automation Portal (TIA Portal)			
		V18 (All versions < V18 Update 3). The affected application			
		contains an improper input validation vulnerability that could			
		allow an attacker to bring the service into a Denial-of-Service state by sending a specifically crafted message to 4004/tcp. The			
	siemens - multiple	corresponding service is auto-restarted after the crash is detected			
CVE-2023-46285	products	by a watchdog.	2023-12-12	7.5	High
	microsoft - multiple	Microsoft Dynamics 365 Finance and Operations Denial of Service			0
CVE-2023-35621	products	Vulnerability	2023-12-12	7.5	High
	microsoft - multiple				
<u>CVE-2023-35622</u>	products microsoft - multiple	Windows DNS Spoofing Vulnerability	2023-12-12	7.5	High
CVE-2023-35638	products	DHCP Server Service Denial of Service Vulnerability	2023-12-12	7.5	High
	microsoft - multiple				0
<u>CVE-2023-35643</u>	products	DHCP Server Service Information Disclosure Vulnerability	2023-12-12	7.5	High
	microsoft - multiple	Windows DPAPI (Data Protection Application Programming			
<u>CVE-2023-36004</u>	products	Interface) Spoofing Vulnerability	2023-12-12	7.5	High
	microsoft -				
CVE-2023-36010	malware_protectio n_platform	Microsoft Defender Denial of Service Vulnerability	2023-12-12	7.5	High
<u>CVL-2023-30010</u>		A flaw was found in Undertow. When an AJP request is sent that	2023-12-12	7.5	півн
		exceeds the max-header-size attribute in ajp-listener, JBoss EAP is			
		marked in an error state by mod_cluster in httpd, causing JBoss			
		EAP to close the TCP connection without returning an AJP			
		response. This happens because mod_proxy_cluster marks the			
		JBoss EAP instance as an error worker when the TCP connection is			
		closed from the backend after sending the AJP request without receiving an AJP response, and stops forwarding. This issue could			
	redhat - multiple	allow a malicious user could to repeatedly send requests that			
CVE-2023-5379	products	exceed the max-header-size, causing a Denial of Service (DoS).	2023-12-12	7.5	High
		IBM Spectrum Scale 5.1.5.0 through 5.1.5.1 uses weaker than			5
	ibm - multiple	expected cryptographic algorithms that could allow an attacker to			
<u>CVE-2022-43843</u>	products	decrypt highly sensitive information. IBM X-Force ID: 239080.	2023-12-14	7.5	High
	-1	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and			
CVE 2022 42042	ibm -	IBM Storage Virtualize 8.3 products use default passwords for a	2022 12 14	7 5	Lliah
<u>CVE-2023-43042</u>	storage_virtualize	privileged user. IBM X-Force ID: 266874. IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3	2023-12-14	7.5	High
	ibm - multiple	through 1.1.9.3 could allow an attacker to obtain a decryption key			
CVE-2023-45184	products	due to improper authority checks. IBM X-Force ID: 268270.	2023-12-14	7.5	High
		@adobe/css-tools versions 4.3.1 and earlier are affected by an	<u> </u>	-	U
		Improper Input Validation vulnerability that could result in a denial			
<u>CVE-2023-48631</u>	adobe - css-tools	of service while attempting to parse CSS.	2023-12-14	7.5	High
	dell - multiple	Dell vApp Manger, versions prior to 9.2.4.x contain an arbitrary file read vulnerability. A remote attacker could potentially exploit this			
CVE-2023-48660	products	vulnerability to read arbitrary files from the target system.	2023-12-14	7.5	High
012 2023 70000	products	sumerasing to read arbitrary mes nom the target system.	2020 12 14	7.5	1.19.1

		DollyApp Manager versions prior to 0.2.4 y contain an			
		Dell vApp Manager, versions prior to 9.2.4.x contain an information disclosure vulnerability. A remote attacker could			
	dell - multiple	potentially exploit this vulnerability leading to obtain sensitive			
CVE-2023-48671	products	information that may aid in further attacks.	2023-12-14	7.5	High
<u>CVL 2023 40071</u>	hp -	Certain HP OfficeJet Pro printers are potentially vulnerable to a	2023 12 14	7.5	111811
	officejet_pro_8730	Denial of Service when sending a SOAP message to the service on			
CVE-2023-4694	_d9l19a_firmware	TCP port 3911 that contains a body but no header.	2023-12-14	7.5	High
012 2020 1001		Multiple WSO2 products have been identified as vulnerable due to	2020 12 11	7.0	
	wso2 -	an XML External Entity (XXE) attack abuses a widely available but			
CVE-2023-6836	api_manager	rarely used feature of XML parsers to access sensitive information.	2023-12-15	7.5	High
	<u></u>	A vulnerability exists on all versions of Ivanti Connect Secure			
	ivanti - multiple	below 22.6R2 where an attacker can send a specific request which			
CVE-2023-39340	products	may lead to Denial of Service (DoS) of the appliance.	2023-12-16	7.5	High
	microsoft - multiple				Ŭ
CVE-2023-36019	products	Microsoft Power Platform Connector Spoofing Vulnerability	2023-12-12	7.4	High
		SAP GUI for Windows and SAP GUI for Java - versions SAP_BASIS			
		755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, allow an			
		unauthenticated attacker to access information which would			
		otherwise be restricted and confidential. In addition, this			
		vulnerability allows the unauthenticated attacker to create Layout			
		configurations of the ABAP List Viewer and with this causing a mild			
	sap - multiple	impact on integrity and availability, e.g. also increasing the			
<u>CVE-2023-49580</u>	products	response times of the AS ABAP.	2023-12-12	7.3	High
	microsoft -				
	azure_connected_	Azure Connected Machine Agent Elevation of Privilege			
CVE-2023-35624	machine_agent	Vulnerability	2023-12-12	7.3	High
	microsoft - multiple				
CVE-2023-36003	products	XAML Diagnostics Elevation of Privilege Vulnerability	2023-12-12	7.3	High
		A vulnerability has been identified in SINEC INS (All versions < V1.0			
		SP2 Update 2). The radius configuration mechanism of affected			
		products does not correctly check uploaded certificates. A			
		malicious admin could upload a crafted certificate resulting in a			
	siemens - multiple	denial-of-service condition or potentially issue commands on			
CVE-2023-48428	products	system level.	2023-12-12	7.2	High
		A vulnerability exists on all versions of Ivanti Connect Secure			
		below 22.6R2 where an attacker impersonating an administrator			
	ivanti - multiple	may craft a specific web request which may lead to remote code			
CVE-2023-41719	products	execution.	2023-12-14	7.2	High
					Ű
		Dell vApp Manager, versions prior to 9.2.4.x contain a command			
		injection vulnerability. A remote malicious user with high			
	dell - multiple	privileges could potentially exploit this vulnerability leading to the			
CVE-2023-48662	products	execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
					Ű
		Dell vApp Manager, versions prior to 9.2.4.x contain a command			
		injection vulnerability. A remote malicious user with high			
	dell - multiple	privileges could potentially exploit this vulnerability leading to the			
CVE-2023-48663	products	execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
		Dell vApp Manager, versions prior to 9.2.4.x contain a command			
		injection vulnerability. A remote malicious user with high			
	dell - multiple	privileges could potentially exploit this vulnerability leading to the			
CVE-2023-48664	products	execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
		Dell vApp Manager, versions prior to 9.2.4.x contain a command			
		injection vulnerability. A remote malicious user with high			
	dell - multiple	privileges could potentially exploit this vulnerability leading to the			
CVE-2023-48665	products	execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
		Due to lack of proper authorization checks in Emarsys SDK for			
		Android, an attacker can call a particular activity and can forward			
		himself web pages and/or deep links without any validation			
		directly from the host application. On successful attack, an			
		attacker could navigate to arbitrary URL including application deep			
CVE-2023-6542	sap - emarsys_sdk	links on the device.	2023-12-12	7.1	High
<u>CVE-2023-6542</u>		An improper access control vulnerability exists in a Huawei			
<u>CVE-2023-6542</u>					
	huawei -	datacom product. Attackers can exploit this vulnerability to obtain			High
	huawei - ar617vw_firmware		2023-12-12	7.1	
		datacom product. Attackers can exploit this vulnerability to obtain	2023-12-12	7.1	
		datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted	2023-12-12	7.1	
		datacom product. Attackers can exploit this vulnerability to obtain partial device information.	2023-12-12	7.1	
		datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted	2023-12-12	7.1	
	ar617vw_firmware	datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2023-12-12	7.1	
	ar617vw_firmware schneider-electric -	datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon	2023-12-12 2023-12-14	7.1	High
<u>CVE-2022-48615</u>	ar617vw_firmware schneider-electric - easy_ups_online_m	datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon service restart when accessed by			High
<u>CVE-2022-48615</u>	ar617vw_firmware schneider-electric - easy_ups_online_m	datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon service restart when accessed by a local and low-privileged attacker.			High
<u>CVE-2022-48615</u>	ar617vw_firmware schneider-electric - easy_ups_online_m onitoring_software	datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon service restart when accessed by a local and low-privileged attacker. SAP Business Objects Web Intelligence - version 420, allows an			High
<u>CVE-2022-48615</u>	ar617vw_firmware schneider-electric - easy_ups_online_m	 datacom product. Attackers can exploit this vulnerability to obtain partial device information. A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon service restart when accessed by a local and low-privileged attacker. SAP Business Objects Web Intelligence - version 420, allows an authenticated attacker to inject JavaScript code into Web 			High

access to. In the worst case, attacker could access data from						
Avulnerability has been identified in LOGO 112/24RCE (All versions >> V8.3), LOGO 12474RCE (All versions >> V8.3), DGOI 230RCE (All versions >> V8.3), LOGOI 2476CE (All versions >> V8.3), LOGOI 24CE (All versions >> V8.3), LOGOI 24RCE (All versions >> V8.3), SIDE Coll 24CE (All versions >> V8.3), LOGOI 24RCE (All versions >> V8.3), SIPLUS LOGOI 124CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 12/2ARCE (All versions >> V8.3), SIDE LOGOI 24CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 24CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 24CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE 2002 44CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE LOGOI 240CE (All versions >> V8.3), SIDE 2002 44CE (All versions <> V8.0), SIDE 2002 44CE (All versions <v8.0), SIDE 2004 44CE (All versions <v< td=""><td></td><td></td><td>access to. In the worst case, attacker could access data from</td><td></td><td></td><td></td></v<></v8.0), </v8.0), </v8.0), </v8.0), </v8.0), 			access to. In the worst case, attacker could access data from			
>= Y8.3), LOGO1 12/24RCE (All versions >= V8.3), LOGO1 200CE (All versions >= V8.3), LOGO1 200CE (All versions >= V8.3), LOGO1 24CE (All versions >= V8.3), LOGO1 24CE (All versions >= V8.3), SIPLUS LOGO1 12/24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.0), SIPLUS LOGO1 24RCE (All versions >= V8.0						
(All versions >= V8.3), LOGO 1230RCE0 (All versions >= V8.3), LOGO 124CE (All versions >= V8.3), LOGO 124CE0 (All versions >= V8.3), LOGO 124CE (All versions >= V8.3), SIDUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 112/24RCE (All versions >= V8.3), SIDUS LOGO 1230RCE0 (All versions >= V8.3), SIPLUS LOGO 1224RCE0 (All versions >= V8.3), SIPLUS LOGO 1230RCE0 (All versions >= V8.3), SIPLUS LOGO 124CE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions >= V8.3), SIPLUS LOGO 124RCE (All versions >= V8.3), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 124RCE0 (All versions <= V8.0), SIPLUS LOGO 1						
LGG01 Z4CE [All versions > W 3], LGG01 Z4CE0 [All versions >> W 3], LGG01 Z4CE0 [All versions >> W 3], SIPLUS LGG01 12/24RCE (All versions >> W 3], SIPLUS LGG01 23/24RCE (All versions >> W 3], SIPLUS LGG01 24/24CE (All versions >= W 3], SCLANCE M3/24 LTE(4G) NAM (All versions <w 24="" 30),="" alv="" m3="" parce="" s<="" sclance="" siple="" siplus="" td=""><td></td><td></td><td></td><td></td><td></td><td></td></w>						
versions >= V8.3), SPLUS LOGO1 12/24RCE0 (All versions >= V8.3), SIPLUS LOGO1 22/24RCE0 (All versions >= V8.3), SIPLUS LOGO1 230RCE (All versions >= V8.3), SIPLUS LOGO1 230RCE0 (All versions >= V8.3), SIPLUS LOGO1 240CE (All versions >= V8.3), SIPLUS LOGO1 24CE0 (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24CE (All versions >= V8.3), SIPLUS LOGO1 24CE0 (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE0 (All versions >= V8.3), SIPLUS LOGO1 24CE0 (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE0 (All versions >= V8.3), SIPLUS LOGO1 24CE0 (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE0 (All versions >= V8.3), SIPLUS LOGO1 24CE0 (22.242784) 064105 CVE-2022-42784 Oba1, firmware times oft + multiple microsoft USBHUB 3.0 Device Driver Remote Code Execution Vulnerability has been identified in RUGGEDCOM RMI224 2023-12-12 6.8 Medium CVE-2023-35629 products Vulnerability has been identified in RUGGEDCOM RMI224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RMI224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RMI224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RMI224 1014 Versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Anne						
CVE-2022-42284 SPRUS LOGOI 12/4RCE (All versions >= V8.3), SIPLUS LOGOI 230RCE (All versions >= V8.3), SIPLUS LOGOI 240C6 (All versions <= V8.0), SCALANCE M3124 LIF(4G) EVALUATE VILLE (All versions <= V8.0), SCALANCE M3124 LIF(4G) EVALUATE VILLE (All versions <= V8.0), SCALANCE M3124 LIF(4G) EVALUATE (All versions <= V8.0), SCALANCE M3124 LIF(4G) EVALUATE (All versions <= V8.0), SCALANCE M376-3 (EVDO) (All versions <= V8.0), SCALANCE M376-3 (EVDO) (All versions <= V8.0), SCALANCE M376-4 (EVALUATE), SCALANCE M376-4 (All versions <= V8.0), SCALANCE M376-4 (All						
CVE-2022-42784 2300EC (All versions >= V8.3), SIPLUS LOGO1 230REC (All versions >= V8.3), SIPLUS LOGO1 24CE (All versions >= V8.3), SIPLUS LOGO1 cv8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), SIPLUS LOGO1 24RCE (All versions >= V8.3), Alfected devices are vulnerable to an electromagnetic fault injection. This could allow an attacker to dump and debug the firmware, including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RM1224 112(46) EU (All versions < V8.0), SCALANCE MB04PB (All versions < V8.0), SCALANCE MB12-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE MB12-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE MB12-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE MB12-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE MB16-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE MB76-3 (EVDO) (All versions < V8.0), SCALANCE MB76-4 (IAM) (All versions < V8.0),						
CVE-2022-42784 Obs1 JERNAGE A vulnerability loss >= V8.3), SIPLUS LOGO1 24RCE (All versions < V8.0), SCLANCE MB12-1 ADSL-ROUTEr (Annex A) (All versions < V8.0), SCLANCE MB12-1 ADSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB16-1 ADSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTEr (Annex B) (All versions < V8.0), SCLANCE (MB26-2 SHDSL-ROUTER (ANNEX 6), SCLANCE (MB26-3 SHDSL-ROUTER (ANNEX 6), SCLANCE (MB26-3 SHDSL-ROUTER (ANNEX 6), SCLANCE (MB26-4), SCLANCE (MB26-2 SHDSL-ROUTER (ANNEX 6), SCLANCE (MB26-4), SCLANCE (MB26-4), SCL						
CVE-2022-42784 24CEC (AII versions >= V8.3), SiPLUS LOGO1 24RCE (AII versions >= V8.3), Affected devices are vulnerable to an electromagnetic fault injection. This could allow an attacker to dump and debug the firmware, including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium CVE-2022-42784 Oba1_firmware Wicrosoft USBHUB 3.0 Device Driver Remote Code Execution 2023-12-12 6.8 Medium CVE-2023-35629 products Vulnerability 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability Ass been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability Ass been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability Ass been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability Ass been identified in RUGGEDCOM RM1224 2014 versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALAN						
CVE-2022-42784 0 ball firmware including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium CVE-2022-42784 Obal firmware ball firmware with chare then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium CVE-2023-35529 products Vulnerability 2023-12-12 6.8 Medium NAM (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 (ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M876-3 (ROV) (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-4 (All) versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0), SCALANCE M876-3 (ROV) (All versions < V8.0), SCALANCE M876-3 (ROV) (All versions < V8.0), SCALANCE M876-3 (ROV) (All versions < V8.0), SCALANCE M876-4 (IAU) (All versions < V8.0), SCAL						
CVE-2022-42784 devices are vulnerable to an electromagnetic fault injection. This could allow an attacker to dump and debug the firmware, including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then allows communication with, and impersonation of a custom certificate allows communication with, and impersonation of a custom certificate allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium CVE-2022-42784 Oba1 firmware Microsoft USBHUB 30 Device Driver Remote Code Execution yulnerability 2023-12-12 6.8 Medium CVE-2023-35629 products Vulnerability has been identified in RUGGEDCOM RM1224 LTE(46) NAM (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B), SCALANCE M812-1 ADSL-Router (Annex B), SCALANCE M812-1 ADSL-Router (Annex B), SCALANCE M812-1 ADSL-Router (Annex S), SCALANCE M812-1 ADSL-ROUTE (All versions < V8.0), SCALANCE M812-1 ADSL-						
CVE-2022-42784 Oba1_firmware including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of 2023-12-12 6.8 Medium CVE-2023-35629 microsoft - multiple products Microsoft USBHUB 3.0 Device Driver Remote Code Execution Vulnerability Ab Device Driver Remote Code Execution 2023-12-12 6.8 Medium CVE-2023-35629 products Vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-3 (EVDO) (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-4 (IAI versions < V8.0), SCALANCE M876-4 (IAI versions < V						
cvE-2022-42784 Oba1_firmware to inject public keys of custom created key pairs which are then allows communication of any device of allows communication with, and impersonation of, any device of the same version. 2023-12-12 6.8 Medium cvE-2022-42784 Oba1_firmware microsoft - multiple Microsoft USBHUB 3.0 Device Driver Remote Code Execution 2023-12-12 6.8 Medium cvE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 products A vulnerability has been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium CVE-2023-35629 product S A vulnerability has been identified in RUGGEDCOM RM1224 2023-12-12 6.8 Medium Vulnerability SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-3 (EWDO) (All versions < V8.0), SCALANCE M876-3 (EWDO) (All versions < V8.0), SCALANCE M876-4 (IAI versions < V8						
siemens - 6ed1052- Inrd08- Dab firmware signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of 2023-12-12 6.8 Medium CVE-2022-42784 Oba1 firmware products Microsoft USBHUB 3.0 Device Driver Remote Code Execution 2023-12-12 6.8 Medium CVE-2023-35629 products Microsoft USBHUB 3.0 Device Driver Remote Code Execution 2023-12-12 6.8 Medium A vulnerability has been identified in RUGGEDCOM RM1224 LTE(46) EU (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M876-3 (EVD) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (LU) (All versions < V8.0), SCALANCE M876-4 (NAM) (All versions < V8.0), SCALANCE M376-3 (ROK) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE M876-4 (NAM) (All versions < V8.0), SCALANCE M376-3 (ROK), SCALANCE M876-4 (RUM) (All versions < V8.0), SCALANCE M876-4 (NAM) (All versions < V8.0), SCALANCE MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM855-1 (EU) (All versions < V8.0), SCALANCE M376-3 (ROK), SCALANCE M376-4 (RUM) (All versions < V8.0), SCALANCE M876-4 (RUMAN) (All versions < V8.0), SCALANCE M30, SCALANCE M876-4 (RUMAN) (All versions < V8.0), SCALANCE M30, S						
CVE-2022-427841md08- Oba1_firmwareallows communication with, and impersonation of, any device of the same version.2023-12-126.8MediumCVE-2023-35629microsoft - multipleMicrosoft USBHUB 3.0 Device Driver Remote Code Execution Vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-3 (EVDO) (All versions < V8.0), SCALANCE M876-3 (INI versions < V8.0), <td></td> <td>ciamons 6ad1052</td> <td></td> <td></td> <td></td> <td></td>		ciamons 6ad1052				
CVE-2022-42784Oba1 firmwarethe same version.2023-12-126.8Mediummicrosoft - multiplemicrosoft USBHUB 3.0 Device Driver Remote Code Execution2023-12-126.8MediumCVE-2023-35629productsA vulnerability as been identified in RUGGEDCOM RM12242023-12-126.8MediumLTE(4G) EU (All versions < V8.0), RUGEDCOM RM1224 LTE(4G)						
CVE-2023-35629productsVulnerability2023-12-126.8MediumA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V8.0), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-2 SHDSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-3 (EVDO) (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M876-4 (Clu) (All versions < V8.0), SCALANCE M876-3 (EVDO) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (LU) (Versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0), SCALANCE M876-4 (LU) (All versions < V8.0), SCALANCE M010856-1 (EU) (All versions < V8.0), SCALANCE SG15 (FI) leversions < V8.0), SCALANCE SG15 FIC (All versions < V8.0), SCALANCE SG15 (All versions < V8.0), SCALANCE SG15 (EU) (All versions < V8.0), SCALANCE SG15 (EU) (All versions < V8.0), SCALANCE M010856-1 (EU) (All versions < V8.0), SCALANCE SG15 (EU) (All versions < V7.2.2), SCALANCE SG15 (EDOM RM122	CVE-2022-42784		· · · ·	2023-12-12	6.8	Medium
A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-3 (ADSL (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-3 (All versions < V8.0), SCALANCE M876-3 (EVD0) (All versions < V8.0), SCALANCE M876-4 (NAM) (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (IQW) (All versions < V8.0), SCALANCE M876-4 (INAM) (All versions < V8.0), SCALANCE MUM353-1 (EU) (All versions < V8.0), SCALANCE MUM356-1 (EU) (All versions < V8.0), SCALANCE MUM356-1 (ROW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update. 2023-12-12 6.7 Medium (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions		microsoft - multiple	Microsoft USBHUB 3.0 Device Driver Remote Code Execution			
LTE(4G) EU (Åll versions < V8.0), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V8.0), SCALANCE M804PB (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-3 (All versions < V8.0), SCALANCE M876-3 (EVDO) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE MM856-1 (EU) (All versions < V8.0), SCALANCE MM856-1 (RoW) (All versions < V8.0), SCALANCE M876-4 (NAW) (All versions < V8.0), SCALANCE MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S010 of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmware VUINerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M81241 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SC	CVE-2023-35629	products		2023-12-12	6.8	Medium
NAM (All versions < V8.0), SCALANCE M804PB (All versions < V8.0),			,			
SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V8.0),						
CVE-2023-49691SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M876-3 (II versions < V8.0), SCALANCE M876-3 (II versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (ROW) (All versions < V8.0), SCALANCE SG15 (All versions < V8.0), SCALANCE SG15 EEC (All versions < V8.0), SCALANCE SG15 (All versions < V8.0), SCALANCE SG15 EEC (All versions < V8.0), SCALANCE SG15 EEC (All versions < V8.0), Scalance and on of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions						
SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V8.0), SCALANCE M826-2 SHDSL-Router (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (LU) (All versions < V8.0), SCALANCE M876-4 (RAM) (All versions < V8.0), SCALANCE M876-4 (RU) (All versions < V8.0), SCALANCE MUM856-1 (ROW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE M104 versions < V8.0), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions						
CVE-2023-49691SCALANCE M826-2 SHDSL-Router (All versions < V8.0), SCALANCE M874-2 (All versions < V8.0), SCALANCE M874-3 (All versions < V8.0), SCALANCE M876-3 (RUK) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0), SCALANCE MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (ROW) (All versions < V8.0), SCALANCE MUM856-1 (ROW) (All versions < V8.0), SCALANCE MUM856-1 (ROW) (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions						
CVE-2023-496912ba2_firmwareSitemens - 6gk6108- value ability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < v7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < v7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions 2023-12-126.7						
V8.0), SCALANCE M876-3 (EVDO) (All versions < V8.0), SCALANCE M876-3 (ROK) (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE M876-4 (All versions < V8.0), SCALANCE MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (RoW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions						
CVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions <						
SCALANCE M876-4 (NAM) (All versions < V8.0), SCALANCE MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (RoW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges 						
MUM853-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (EU) (All versions < V8.0), SCALANCE MUM856-1 (RoW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <			versions < V8.0), SCALANCE M876-4 (EU) (All versions < V8.0),			
(All versions < V8.0), SCALANCE MUM856-1 (RoW) (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwaresystem level after a successful IP address update.2023-12-126.7MediumA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions						
V8.0), SCALANCE S615 (All versions < V8.0), SCALANCE S615 EEC (All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
(All versions < V8.0). An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions 6.7Medium						
Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumCVE-2023-496912ba2_firmwareA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
4am00- 2ba2_firmwarecould allow malicious local administrators to issue commands on system level after a successful IP address update.2023-12-126.7MediumA vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
CVE-2023-49691 2ba2_firmware system level after a successful IP address update. 2023-12-12 6.7 Medium A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G)		-				
LTE(4G) EU (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <	CVE-2023-49691			2023-12-12	6.7	Medium
NAM (All versions < V7.2.2), SCALANCE M804PB (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
V7.2.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
V7.2.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions <						
1/7 2 2) SCALANCE M916 1 ADSL Bouter (Append A) (All versions 4						
V7.2.2), SCALANCE WIGTO-T ADSL-ROULET (AIMEX A) (AII VEISIONS <			V7.2.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions <			
V7.2.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions <						
V7.2.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.2.2), SCALANCE M874-2 (All versions < V7.2.2), SCALANCE M874-3 (All						
versions < V7.2.2), SCALANCE M876-3 (EVDO) (All versions <						
V7.2.2), SCALANCE M876-3 (ROK) (All versions < V7.2.2),						
SCALANCE M876-4 (All versions < V7.2.2), SCALANCE M876-4 (EU)						
(All versions < V7.2.2), SCALANCE M876-4 (NAM) (All versions <						
V7.2.2), SCALANCE MUM853-1 (EU) (All versions < V7.2.2), SCALANCE MUM856-1 (EU) (All versions < V7.2.2), SCALANCE						
MUM856-1 (RoW) (All versions < V7.2.2), SCALANCE						
versions < V7.2.2), SCALANCE S615 EEC (All versions < V7.2.2). An						
Improper Neutralization of Special Elements used in an OS						
Command with root privileges vulnerability exists in the parsing of						
siemens - 6gk6108-the IPSEC configuration. This could allow malicious local4am00-administrators to issue commands on system level after a new						
CVE-2023-496922ba2_firmwareconnection is established.2023-12-126.7Medium				2023-12-12	6.7	Medium
Jenkins OpenId Connect Authentication Plugin 2.6 and earlier	CVE-2023-49692					
stores a password of a local user account used as an anti-lockout	<u>CVE-2023-49692</u>	•				
feature in a recoverable format, allowing attackers with access to	<u>CVE-2023-49692</u>					
	<u>CVE-2023-49692</u>		feature in a recoverable format, allowing attackers with access to			
	<u>CVE-2023-49692</u>		feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text			
CVE 2023 50/70 Jenkins Openia Jenkins 2023 12 13 0.7 The NSS code used for checking PKCS#1 v1.5 was leaking The NSS code used for checking PKCS#1 v1.5 was leaking		ienkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to	2023-12-13	6.7	Medium
information useful in mounting Bleichenbacher-like attacks. Both	<u>CVE-2023-49692</u> <u>CVE-2023-50770</u>	jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins.	2023-12-13	6.7	Medium
the overall correctness of the padding as well as the length of the		jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both	2023-12-13	6.7	Medium
		jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the	2023-12-13	6.7	Medium
		jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By	2023-12-13	6.7	Medium
v1.5 ciphertext (for example, to decrypt a TLS session that used		jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By sending large number of attacker-selected ciphertexts, the	2023-12-13	6.7	Medium
RSA key exchange), or forge a signature using the victim's key. The		jenkins - openid	feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By sending large number of attacker-selected ciphertexts, the attacker would be able to decrypt a previously intercepted PKCS#1	2023-12-13	6.7	Medium
CVE-2023-4421mozilla - nssissue was fixed by implementing the implicit rejection algorithm, in2023-12-126.5Medium	<u>CVE-2023-50770</u>		feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins. The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By sending large number of attacker-selected ciphertexts, the attacker would be able to decrypt a previously intercepted PKCS#1 v1.5 ciphertext (for example, to decrypt a TLS session that used RSA key exchange), or forge a signature using the victim's key. The			

		which the NSS returns a deterministic random message in case invalid padding is detected, as proposed in the Marvin Attack paper. This vulnerability affects NSS < 3.61.			
<u>CVE-2023-35636</u>	microsoft - multiple products microsoft - multiple	Microsoft Outlook Information Disclosure Vulnerability	2023-12-12	6.5	Medium
<u>CVE-2023-35642</u>	products	Internet Connection Sharing (ICS) Denial of Service Vulnerability Improper access control in Zoom Mobile App for iOS and Zoom	2023-12-12	6.5	Medium
<u>CVE-2023-43585</u>	zoom - multiple products	SDKs for iOS before version 5.16.5 may allow an authenticated user to conduct a disclosure of information via network access. Improper authentication in some Zoom clients before version	2023-12-13	6.5	Medium
CVE-2023-49646	zoom - multiple products	5.16.5 may allow an authenticated user to conduct a denial of service via network access.	2023-12-13	6.5	Medium
<u>CVE-2023-21751</u>	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-12-14	6.5	Mediun
<u>CVL-2023-21731</u>		IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 is vulnerable to having its key for an encrypted password decoded. By somehow gaining access to the encrypted	2023-12-14	0.5	Meulun
<u>CVE-2023-45182</u>	ibm - multiple products	password, a local attacker could exploit this vulnerability to obtain the password to other systems. IBM X-Force ID: 268265. SAP Solution Manager - version 720, allows an authorized attacker	2023-12-14	6.5	Mediun
<u>CVE-2023-49587</u>	sap - solution_manager	to execute certain deprecated function modules which can read or modify data of same or other component without user interaction over the network.	2023-12-12	6.4	Mediun
	apple - multiple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, macOS Ventura 13.6.3, tvOS 17.2, iOS 16.7.3 and iPadOS 16.7.3, macOS Monterey 12.7.2. An app may be able to			
<u>CVE-2023-42914</u>	products	break out of its sandbox. An OS command injection vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated API user to	2023-12-12	6.3	Mediun
<u>CVE-2023-6792</u>	paloaltonetworks - multiple products	disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	2023-12-13	6.3	Mediur
<u>CVE-2023-42479</u>	sap - multiple products	An unauthenticated attacker can embed a hidden access to a Biller Direct URL in a frame which, when loaded by the user, will submit a cross-site scripting request to the Biller Direct system. This can result in the disclosure or modification of non-sensitive information.	2023-12-12	6.1	Mediur
	san multiple	The SAP HCM (SMART PAYE solution) - versions S4HCMCIE 100, SAP_HRCIE 600, SAP_HRCIE 604, SAP_HRCIE 608, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity			
<u>CVE-2023-49577</u>	sap - multiple products	of the application. In Red Hat Advanced Cluster Security (RHACS), it was found that	2023-12-12	6.1	Mediun
	redhat - multiple	some security related HTTP headers were missing, allowing an attacker to exploit this with a clickjacking attack. An attacker could exploit this by convincing a valid RHACS user to visit an attacker- controlled web page, that deceptively points to valid RHACS endpoints, hijacking the user's account permissions to perform			
<u>CVE-2023-4958</u>	products	other actions. A vulnerability has been identified in Opcenter Quality (All	2023-12-12	6.1	Mediur
	siemens - multiple	versions), SIMATIC PCS neo (All versions < V4.1), SINUMERIK Integrate RunMyHMI /Automotive (All versions), Totally Integrated Automation Portal (TIA Portal) V14 (All versions), Totally Integrated Automation Portal (TIA Portal) V15.1 (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected applications that could allow an attacker to inject arbitrary JavaScript code. The code could be potentially executed later by			
<u>CVE-2023-46282</u>	products	another (possibly privileged) user. Jenkins OpenId Connect Authentication Plugin 2.6 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform	2023-12-12	6.1	Mediun
<u>CVE-2023-50771</u>	jenkins - openid	phishing attacks. A DOM-Based cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a remote attacker to execute a JavaScript payload in the context of an administrator's browser	2023-12-13	6.1	Mediun
<u>CVE-2023-6790</u>	paloaltonetworks - multiple products	when they view a specifically crafted link to the PAN-OS web interface.	2023-12-13	6.1	Mediur
CVE-2023-46750	apache - multiple products	URL Redirection to Untrusted Site ('Open Redirect') vulnerability when "form" authentication is used in Apache Shiro. Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+.	2023-12-14	6.1	Mediun

CVE 2022 6828	wso2 - multiple	Reflected XSS vulnerability can be exploited by tampering a request parameter in Authentication Endpoint. This can be	2022 12 15	6.1	Medium
<u>CVE-2023-6838</u>	products	performed in both authenticated and unauthenticated requests. Design document functions which receive a user http request object may expose authorization or session cookie headers of the user who accesses the document.	2023-12-15	6.1	Medium
		These design document functions are: * list			
		 * show * rewrite * update 			
		An attacker can leak the session component using an HTML-like output, insert the session as an external resource (such as an image), or store the credential in a _local document with an "update" function.			
		For the attack to succeed the attacker has to be able to insert the design documents into the database, then manipulate a user to access a function from that design document.			
<u>CVE-2023-45725</u>	apache - couchdb	Workaround: Avoid using design documents from untrusted sources which may attempt to access or manipulate request object's headers	2023-12-13	5.7	Medium
		A null pointer dereference vulnerability was found in dpll_pin_parent_pin_set() in drivers/dpll/dpll_netlink.c in the Digital Phase Locked Loop (DPLL) subsystem in the Linux kernel.			
<u>CVE-2023-6679</u>	linux - linux_kernel	This issue could be exploited to trigger a denial of service. The issue was addressed with improved memory handling. This	2023-12-11	5.5	Medium
<u>CVE-2023-42883</u>	apple - multiple products	issue is fixed in Safari 17.2, macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, tvOS 17.2, iOS 16.7.3 and iPadOS 16.7.3. Processing an image may lead to a denial-of-service.	2023-12-12	5.5	Medium
		This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.2, iOS 17.2			
<u>CVE-2023-42884</u>	apple - multiple products	and iPadOS 17.2, macOS Ventura 13.6.3, tvOS 17.2, iOS 16.7.3 and iPadOS 16.7.3. An app may be able to disclose kernel memory. An authentication issue was addressed with improved state	2023-12-12	5.5	Mediun
	apple - multiple	management. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. An app may be able to			
<u>CVE-2023-42891</u>	products	monitor keystrokes without user permission. This issue was addressed with improved redaction of sensitive	2023-12-12	5.5	Medium
<u>CVE-2023-42894</u>	apple - multiple products	information. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. An app may be able to access information about a user's contacts.	2023-12-12	5.5	Medium
	apple - multiple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2, watchOS 10.2, iOS 17.2 and iPadOS 17.2, tvOS 17.2. Processing an image may lead to arbitrary			
<u>CVE-2023-42898</u>	products	code execution. The issue was addressed with improved checks. This issue is fixed	2023-12-12	5.5	Medium
<u>CVE-2023-42900</u>	apple - macos	in macOS Sonoma 14.2. An app may be able to access user- sensitive data.	2023-12-12	5.5	Medium
CVE-2023-42919	apple - multiple	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, macOS Ventura 13.6.3, iOS 16.7.3 and iPadOS 16.7.3, macOS Monterey 12.7.2. An app	2023-12-12	5.5	Medium
<u>CVE-2023-42919</u>	products	may be able to access sensitive user data. This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, macOS Ventura 13.6.3, iOS 16.7.3 and iPadOS	2023-12-12	5.5	Wedluff
<u>CVE-2023-42922</u>	apple - multiple products	16.7.3, macOS Monterey 12.7.2. An app may be able to read sensitive location information.	2023-12-12	5.5	Medium
<u>CVE-2023-42924</u>	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3. An app may be able to access sensitive user data. A logic issue was addressed with improved checks. This issue is	2023-12-12	5.5	Mediun
<u>CVE-2023-42932</u>	apple - multiple products	fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. An app may be able to access protected user data. A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) (All versions < V19). An information disclosure vulnerability could	2023-12-12	5.5	Mediur
	siemens -	allow a local attacker to gain access to the access level password of the SIMATIC S7-1200 and S7-1500 CPUs, when entered by a legitimate user in the hardware configuration of the affected			
CVE-2022-46141	simatic_step_7 microsoft - multiple	application.	2023-12-12	5.5	Medium
CVE-2023-35635	products	Windows Kernel Denial of Service Vulnerability	2023-12-12	5.5	Medium

		Adobe InDesign versions 19.0 (and earlier) and 17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the			
<u>CVE-2023-47076</u>	adobe - multiple products	current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
	adaba multinla	Adobe InDesign versions 19.0 (and earlier) and 17.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a vistim must energy and			
CVE-2023-47077	adobe - multiple products	this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
		Adobe Prelude versions 22.6 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious			
<u>CVE-2023-44362</u>	adobe - prelude	file.	2023-12-13	5.5	Medium
<u>CVE-2023-47061</u>	adobe - dimension	Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.10 and earlier are affected by an	2023-12-13	5.5	Medium
CVE-2023-47062	adobe - dimension	out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
		Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires			
<u>CVE-2023-47078</u>	adobe - dimension	user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires	2023-12-13	5.5	Medium
CVE-2023-47079	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-47080	adobe - substance_3d_stag er	Adobe Substance 3D Stager versions 2.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-47081	adobe - substance_3d_stag er	Adobe Substance 3D Stager versions 2.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-48635	adobe - multiple products	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
	adobe - substance_3d_desi	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in			
<u>CVE-2023-48636</u>	gner	that a victim must open a malicious file.	2023-12-13	5.5	Medium
	adobe - substance_3d_desi	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in			
<u>CVE-2023-48637</u>	gner adobe -	that a victim must open a malicious file. Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	2023-12-13	5.5	Medium
<u>CVE-2023-48638</u>	substance_3d_desi gner microsoft - multiple	such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Microsoft Dynamics 365 (on-premises) Cross-site Scripting	2023-12-13	5.5	Medium
CVE-2023-36020	products	Vulnerability	2023-12-12	5.4	Medium
CVE-2023-41673	fortinet - multiple products	An improper authorization vulnerability [CWE-285] in Fortinet FortiADC version 7.4.0 and before 7.2.2 may allow a low privileged	2023-12-13	5.4	Medium

		user to read or backup the full system configuration via HTTP or			
		HTTPS requests. A improper neutralization of input during web page generation			
		('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and			
		4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0			
	fortingt multiple	through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.4 allows attacker to execute unauthorized code or commands via			
CVE-2023-41844	fortinet - multiple products	crafted HTTP requests in capture traffic endpoint.	2023-12-13	5.4	Medium
<u>CVL 2023 41044</u>	products	An improper neutralization of input during web page generation	2023 12 13	5.4	Wiedlah
		('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and			
		4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0			
	fortinet - multiple	through 3.2.4 and 3.1.0 through 3.1.5 allows attacker to execute	2022 12 12	F 4	Madium
<u>CVE-2023-45587</u>	products	unauthorized code or commands via crafted HTTP requests Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-	2023-12-13	5.4	Medium
		03 and earlier allow attackers with Overall/Read permission to			
	jenkins -	send an HTTP request to an attacker-specified URL and parse the			
CVE-2023-50767	nexus_platform	response as XML.	2023-12-13	5.4	Medium
		A flaw was found in Keycloak that prevents certain schemes in			
		redirects, but permits them if a wildcard is appended to the token.			
	redhat -	This issue could allow an attacker to submit a specially crafted request leading to cross-site scripting (XSS) or further attacks. This			
CVE-2023-6134	single_sign-on	flaw is the result of an incomplete fix for CVE-2020-10748.	2023-12-14	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-47064	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>UVL 2023-47004</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	J. 4	weuluit
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-47065</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48440	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adobe - multiple	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
CVE-2023-48442	products	containing the vulnerable field.	2023-12-15	5.4	Medium
	p	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
01/5 2022 40442	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45	F 4	
<u>CVE-2023-48443</u>	products	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Medium
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
<u>CVE-2023-48444</u>	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48445	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are	_		
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 4044C	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45	F 4	N/a-l:
<u>CVE-2023-48446</u>	products	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Mediun
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48447</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
	a de la companya de la	low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 40440	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45	Γ 4	Madim
<u>CVE-2023-48448</u>	products	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Mediun
	adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		- an electron by a cross site sempting (DOM-Dased Ass) VUINE ADMILY. I	1	1	1

		referencing a vulnerable page, malicious JavaScript content may			
		be executed within the context of the victim's browser.			
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48450</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48451	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	•	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48452	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVL 2023 40452</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.4	Wiedlahr
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48453	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48454	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
	adobe - multiple	low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48455	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	p	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48456	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48457	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48458	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	products	Adobe Experience Manager versions 6.5.18 and earlier are	2020 12 10	511	meanum
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48459</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48460	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adoba multinla	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48461	adobe - multiple products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may	2023-12-15	5 4	Medium
<u>CVE-2023-48461</u>	adobe - multiple products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48461</u>	•	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may	2023-12-15	5.4	Medium
<u>CVE-2023-48461</u>	•	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-15	5.4	Medium
	products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
	products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15 2023-12-15	5.4	Medium
	products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are			
	products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	products adobe - multiple products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
<u>CVE-2023-48462</u>	products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
<u>CVE-2023-48462</u>	adobe - multiple products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48462</u>	adobe - multiple products adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If	2023-12-15	5.4	Medium
<u>CVE-2023-48462</u>	adobe - multiple products adobe - multiple products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-15	5.4	Medium
<u>CVE-2023-48461</u> <u>CVE-2023-48462</u> <u>CVE-2023-48463</u>	adobe - multiple products adobe - multiple products adobe - multiple	 affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. 	2023-12-15 2023-12-15	5.4	Medium
<u>CVE-2023-48462</u>	adobe - multiple products adobe - multiple products	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-15	5.4	Medium

		a low-privileged attacker is able to convince a victim to visit a URL			
		referencing a vulnerable page, malicious JavaScript content may			
		be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48466	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48467	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
<u>eve 2023 10107</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.1	Wiedian
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48468</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48469	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48470</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48471	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
012 2020 10171	products	Adobe Experience Manager versions 6.5.18 and earlier are	2020 22 20	5	meana
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48472</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48473	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48474	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48475	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
	·	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45		
CVE-2023-48476	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48477	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48478</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48479	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
	p. 00000	Adobe Experience Manager versions 6.5.18 and earlier are	10	5.1	
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48480	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium

		Adobe Experience Manager versions 6.5.18 and earlier are			
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
affected by a stored Cr could be abused by a la scripts into vulnerable executed in a victim's b containing the vulneraCVE-2023-48481productsadobe - multiple productsAdobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the Adobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the Adobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the Adobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the adobe - multiple productsCVE-2023-48483productsAdobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the adobe Experience Mar affected by a Cross-site a low-privileged attack referencing a vulnerab be executed within the adobe Experience Mar affected by a Cross-site a low-privileged attack		executed in a victim's browser when they browse to the page			
CVE-2023-48481	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 49492	•	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-46462</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weulum
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48483	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adaha multinla	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48484	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVL-2023-40404</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2025-12-15	5.4	wearan
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48485	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48486	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVL-2023-48480</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weaturn
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48487	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 49499	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48488</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weaturn
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48489	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	and a local second second	a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48490	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2025-46490</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weaturn
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48491	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 40402	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45	F 4	Maali
<u>CVE-2023-48492</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48493	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	·	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may		_	
<u>CVE-2023-48494</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48495	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u> </u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12-13	J. 4	wiculum
	adobe - multiple	affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			

		referencing a vulnerable page, malicious JavaScript content may			
		be executed within the context of the victim's browser.			
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48497	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
	adobe - multiple	low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48498	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	·	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48499	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVL-2023-40455</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2025-12-15	5.4	Wealdin
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48500</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48501	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48502	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	·	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adaha multinla	scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-48503	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVL 2023 40303</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.4	Wiediam
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-48504	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2025-46504</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weaturn
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
<u>CVE-2023-48505</u>	products	containing the vulnerable field.Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Medium
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
<u>CVE-2023-48506</u>	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48507	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48508	products	containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adologija (1971)	a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2022 40500	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2022 12 15	E /	Madium
CVE-2023-48509	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Medium
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
		be executed within the context of the victim's browser.			

		Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
<u>CVE-2023-48511</u>	adobe - multiple products	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
<u>CVE-2023-48512</u>	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediun
CVE-2023-48513	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediun
CVE-2023-48513	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediun
CVE-2022-48515	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	2022-12-15	5.4	Mediun
<u>CVE-2023-48515</u>	products	containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	ivieulun
<u>CVE-2023-48516</u>	adobe - multiple products	affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	2023-12-15	5.4	Mediun
CVE-2023-48517	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48517</u>	adobe - multiple products adobe - multiple	 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 	2023-12-15	5.4	Mediun
<u>CVE-2023-48519</u>	products	containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	2023-12-15	5.4	Mediun
<u>CVE-2023-48520</u>	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48521</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48522</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48523</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediun

		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-48524	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.1	meanan
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48525</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48526</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48527	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48528	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	Б Л	Mediun
<u>CVE-2023-48528</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	weatur
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
<u>CVE-2023-48529</u>	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48530	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adobe - multiple	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
CVE-2023-48531	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
	I	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 48522	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may	2022 12 15	F 4	Madius
<u>CVE-2023-48532</u>	adobe - multiple products	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
<u>CVE-2023-48532</u>	•	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are 	2023-12-15	5.4	Mediur
<u>CVE-2023-48532</u>	•	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that 	2023-12-15	5.4	Mediun
<u>CVE-2023-48532</u>	•	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are 	2023-12-15	5.4	Mediun
	products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page 			
	products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. 	2023-12-15 2023-12-15	5.4	
<u>CVE-2023-48532</u> <u>CVE-2023-48533</u>	products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are 			
	products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that 			
	products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 			
	products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 			
<u>CVE-2023-48533</u>	products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 			Mediun
	products adobe - multiple products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are 	2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u>	products adobe - multiple products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 	2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL 	2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may 	2023-12-15 2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. 	2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are 	2023-12-15 2023-12-15	5.4	Mediur
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. 	2023-12-15 2023-12-15	5.4	Mediur
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u>	products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 	2023-12-15 2023-12-15	5.4	Mediur
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u>	adobe - multiple products adobe - multiple products adobe - multiple products	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. 	2023-12-15 2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u> <u>CVE-2023-48535</u>	adobe - multiple products adobe - multiple products adobe - multiple products adobe - multiple	 a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript	2023-12-15 2023-12-15 2023-12-15	5.4	Mediur
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u> <u>CVE-2023-48535</u>	adobe - multiple products adobe - multiple products adobe - multiple products adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browse	2023-12-15 2023-12-15 2023-12-15	5.4	Mediun
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u> <u>CVE-2023-48535</u>	adobe - multiple products adobe - multiple products adobe - multiple products adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Stored Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site S	2023-12-15 2023-12-15 2023-12-15	5.4	Mediun Mediun Mediun Mediun
<u>CVE-2023-48533</u> <u>CVE-2023-48534</u> <u>CVE-2023-48535</u>	adobe - multiple products adobe - multiple products adobe - multiple products adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browse	2023-12-15 2023-12-15 2023-12-15	5.4	Mediun

		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48538	products	containing the vulnerable field.	2023-12-15	5.4	Medium
	•	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48539	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48540	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
	p	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48541	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page	2022 42 45		
CVE-2023-48542	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48543	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
	p. 000000	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48544	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adobe - multiple	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
CVE-2023-48545	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
<u>CVL-2023-48343</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weulun
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48546	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page		-	
CVE-2023-48547	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adobe - multiple	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
CVE-2023-48548	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
	p. 000005	Adobe Experience Manager versions 6.5.18 and earlier are	2020 12 13	5.7	meanu
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48549	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	and a large state of the second se	executed in a victim's browser when they browse to the page			
	adobe - multiple		2022 1		
CVE-2023-48550	products	containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48550</u>	•	containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	2023-12-15	5.4	Mediun

		scripts into vulnerable form fields. Malicious JavaScript may be			
		executed in a victim's browser when they browse to the page			
		containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
executed in containing to containing to Adobe Expect 		scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-48552 products adobe - multipl products CVE-2023-48553 products adobe - multipl adobe - multipl		executed in a victim's browser when they browse to the page			
CVE-2023-48552	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adaha multinla	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
C\/F-2023-48553	•	containing the vulnerable field.	2023-12-15	5.4	Mediu
<u>CVL 2023 10333</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.1	Inculu
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48554	products	containing the vulnerable field.	2023-12-15	5.4	Mediu
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	adobe - multiple	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
CVE-2023-48555	products	containing the vulnerable field.	2023-12-15	5.4	Mediu
<u>CVL 2023 10333</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023 12 13	5.1	meana
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48556</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediu
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
CVE-2023-48557	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediu
<u>CVE-2023-46337</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	weului
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48558	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page	2022 42 45	F 4	Madiu
CVE-2023-48559	products	containing the vulnerable field.	2023-12-15	5.4	Mediu
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48560	products	containing the vulnerable field.	2023-12-15	5.4	Mediu
	•	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
<u>CVE-2023-48561</u>	products	containing the vulnerable field.	2023-12-15	5.4	Mediu
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48562	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
	P - more	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48563	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
	odaha	affected by a stored Cross-Site Scripting (XSS) vulnerability that			
CVE-2023-48564	adobe - multiple	could be abused by a low-privileged attacker to inject malicious	2022 42 45		NA!'
ALLA AVELA	products	scripts into vulnerable form fields. Malicious JavaScript may be	2023-12-15	5.4	Mediur

		executed in a victim's browser when they browse to the page containing the vulnerable field.			
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	adobe - multiple	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48565	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
	·	Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48566	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
<u>CVL-2023-48300</u>	products	Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-13	5.4	Weului
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
	l	a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 12 15	F 4	Madium
<u>CVE-2023-48567</u>	products	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Mediur
		affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If			
		a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48568	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48569	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48570	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
		scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48571	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48572	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious			
	l	scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48573	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48574	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
	l	affected by a stored Cross-Site Scripting (XSS) vulnerability that			
	l	could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48575	products	containing the vulnerable field.	2023-12-15	5.4	Mediun
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48576	products	containing the vulnerable field.	2023-12-15	5.4	Mediur
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by a stored Cross-Site Scripting (XSS) vulnerability that			
		could be abused by a low-privileged attacker to inject malicious			
	1	scripts into vulnerable form fields. Malicious JavaScript may be			
	adobe - multiple	executed in a victim's browser when they browse to the page			
CVE-2023-48577	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediur
CVE-2023-48577	•	executed in a victim's browser when they browse to the pagecontaining the vulnerable field.Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Mediun

		scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.			
<u>CVE-2023-48579</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Mediun
<u>CVE-2023-48580</u>	adobe - multiple products	 affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that 	2023-12-15	5.4	Mediur
<u>CVE-2023-48581</u>	adobe - multiple products	could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediur
CVE-2023-48582	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediur
<u>2vt 2023-40302</u>	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may	2023-12-13	J. 4	mediul
<u>CVE-2023-48583</u>	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
<u>CVE-2023-48584</u>	adobe - multiple products	 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that 	2023-12-15	5.4	Mediur
<u>CVE-2023-48585</u>	adobe - multiple products	 could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious 	2023-12-15	5.4	Mediur
<u>CVE-2023-48586</u>	adobe - multiple products	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Mediur
<u>CVE-2023-48587</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
<u>CVE-2023-48588</u>	products	containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-15	5.4	Mediur
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 42 45	F 4	NA - 11
<u>CVE-2023-48589</u> <u>CVE-2023-48590</u>	products adobe - multiple products	 be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL 	2023-12-15 2023-12-15	5.4	Mediur
<u>CVE-2023-48591</u>	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Mediur
<u>CVE-2023-48592</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious	2023-12-15	5.4	Mediur

executed in a victim's browser when they browse to the page containing the vulnerable field.Image: containing the vulnerable field.adobe - multiple cvE-2023-48593Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48594Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48594Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48595Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to
Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable from fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 CVE-2023-48594 products Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48595 adobe - multiple products Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48595 adobe - multiple products Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48595 adobe - multiple containing the vulnerable field. 2023-12-15 5.4 <
cvE-2023-48593could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4cVE-2023-48594Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cVE-2023-48594productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48595productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-15<
cvE-2023-48593scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4cvE-2023-48593Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cvE-2023-48594productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cvE-2023-48594productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cvE-2023-48595productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cvE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4cvE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged at
CVE-2023-48593 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 VE-2023-48594 Products Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 VE-2023-48595 adobe - multiple products executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 Adobe - multiple executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 Adobe - multiple executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 Adobe - multiple executed in a victim's browser whent they browse to the page containing the vulnerable fi
Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 CVE-2023-48594 products Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page cortaining the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48595 products Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48595 Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48596 products Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable field. 2023-12-15 5.4 QVE-2023-48596 products Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-p
could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48594Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page
adobe - multiple (CVE-2023-48594scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4(VE-2023-48595adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4(VE-2023-48595adobe - multiple productscontaining the vulnerable field.2023-12-155.4(VE-2023-48596adobe - multiple productscontaining the vulnerable field.2023-12-155.4(VE-2023-48596adobe - multiple productscontaining the vulnerable field.2023-12-155.4(VE-2023-48596adobe - multiple productscontaining the vulnerable field.2023-12-155.4(VE-2023-48596productscontaining the vulnerable field.2023-12-155.4(VE-2023-48597productscontaining the vulnerable field.2023-12-155.4(VE-2023-48597productscontaining the vulnerable field.2023-12-155.4(VE-2023-48597productscontaining the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page2023-12-155.4
adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48594Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they forwse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page conta
Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596adobe - multiple productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page cortaining the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2023-48595affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48595Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48596Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48597productsCotaining the vulnerable field.2023-12-155.4CVE-2023-48597productscotaining the vulnerable field.2023-12-155.4CVE-2023-48598adobe - multiple productsscripts into vulnerable field.2023-12-155.4CVE-2023-48598productscotaining the vulnerable field.2023-12-155.4CVE-2023-48598productscotaining the vulnerable field.2023-12-15 </td
cvE-2023-48595could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48595Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48596Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48596productscontaining the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598adobe - multiple executed in a victim's browser
CVE-2023-48595adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598adobe - multiple productscontaining the vulnerable field. </td
CVE-2023-48595productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597adobe - multiple productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaS
Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the pag
CVE-2023-48596could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48597adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-
cVE-2023-48596scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe - multiple affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4Adobe - multiple adobe - multiple adobe - multiple productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48598adobe - multiple affected by a tored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vul
adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48596Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48597productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4
Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe - multiple productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If2023-12-155.4
CVE-2023-48597adobe - multiple productsaffected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If5.4
cvE-2023-48597could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48597Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page 2023-12-155.4CVE-2023-48598Adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-15CVE-2023-48598productscontaining the vulnerable field.2023-12-15CVE-2023-48598productscontaining the vulnerable field.2023-12-15Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If5.4
adobe - multiple productsexecuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If5.4
CVE-2023-48597productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If5.4
CVE-2023-48598affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. IfAdobe Experience Manager versions 6.5.18Adobe Experience Manag
CVE-2023-48598could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple script in a victim's browser when they browse to the page 2023-12-155.4
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If11
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
a low-privileged attacker is able to convince a victim to visit a URL
adobe - multiplereferencing a vulnerable page, malicious JavaScript content mayCVE-2023-48599productsbe executed within the context of the victim's browser.2023-12-155.4
Adobe Experience Manager versions 6.5.18 and earlier are 2023 12 13 3.4
affected by a stored Cross Site Seriating (VCC) will probability that
affected by a stored Cross-Site Scripting (XSS) vulnerability that
could be abused by a low-privileged attacker to inject malicious
could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier areAdobe Experience Manager versions 6.5.18 and earlier areCVE-2023-12-15CVE-2023-12-15
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL11
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that5.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsbe executed within the context of the victim's browser.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious5.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that5.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601ProductsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601ProductsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsbe executed within the context of the victim's browser.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page2023-12-155.4CVE-2023-48602productscontaining the vulnerable field.2023-12-155.4CVE-2023-48602productscontaining the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page2023-12-155.4C
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields.2023-12-155.4
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsbe executed within the context of the victim's browser.2023-12-155.4Adobe - multiple adobe - multipleaffected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productscontaining the vulnerable field.2023-12-155.4CVE-2023-48603productscontaining the vulnerable field.2023-12-155.4CVE-2023-48603productscontaining the vulnerable form fields. M
cvE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be excuted in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be excuted in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields.2023-12-155.4CVE-2023-48603productsAdobe Experience Manager versions 6.5.18 and ea
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convice a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsbe executed within the context of the victim's browser.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productscontaining the vulnerable field.2023-12-155.4VE-2023-48603productscontaining the vulnerable field.2023-12-155.4CVE-2023-48603productscontaining the vulnerable field.2023-12-155.4CVE-2023-48603productscontaining the vulnerable field.2023-12-155.4CVE-2023-48603productscontaining the
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48603productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page prod
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48603products
CVE-2023-48600could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48600Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.2023-12-155.4CVE-2023-48601productsbe executed within the context of the victim's browser.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48602productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable field.2023-12-155.4CVE-2023-48603productsAdobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vul
could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be
l a low-privileged attacker is able to convince a victim to visit a URL
a low-privileged attacker is able to convince a victim to visit a URL
La low-privileged attacker is able to convince a victim to visit a LIRI
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple products executed in a victim's browser when they browse to the page containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerability. Ifadobe - multiple containing the vulnerable field.
CVE-2023-48598could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. IfAdobe Experience Manager versions 6.5.18Adobe Experience Manager versions 6.5.18
CVE-2023-48598could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. IfAdobe Experience Manager versions 6.5.18Adobe Experience Manager versions 6.5.18
CVE-2023-48598could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4CVE-2023-48598Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. IfAdobe Experience Manager versions 6.5.18Adobe Experience Manager versions 6.5.18
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerability. Ifadobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
cvE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
CVE-2023-48598scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. Ifadobe - multiple containing the vulnerable field.adobe - multiple containing the vulnerable field.
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 products Adobe Experience Manager versions 6.5.18 and earlier are 2023-12-15 5.4 Adobe Experience Manager versions (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If Image: Comparison of the page of th
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 products Adobe Experience Manager versions 6.5.18 and earlier are 2023-12-15 5.4 Adobe Experience Manager versions (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If Image: Comparison of the page of th
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 products Adobe Experience Manager versions 6.5.18 and earlier are 2023-12-15 5.4 Adobe Experience Manager versions (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If Image: Comparison of the page of th
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
CVE-2023-48598productscontaining the vulnerable field.2023-12-155.4Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If44
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
adobe - multiple executed in a victim's browser when they browse to the page 2023-12-15 5.4 CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If Image: Comparison of the page
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
CVE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 5.4
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If b
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If b
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If b
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If b
VE-2023-48598 products containing the vulnerable field. 2023-12-15 5.4 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If b
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If
a low-privileged attacker is able to convince a victim to visit a URL
adobe - multiple I reterencing a vulnerable page malicious JavaScript content mav
offected by a stared Cross Cite Coninting (VCC) will even billing that
Auove Experience initializer versions 0.3.10 ditu earlier are

		Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
CVE-2023-48606	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48607	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-48609	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48610	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48010</u>	·	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-13	5.4	Medium
CVE-2023-48611	adobe - multiple products	referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48612</u>	products	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Medium
<u>CVE-2023-48613</u>	adobe - multiple products	affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
	adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
<u>CVE-2023-48614</u>	products adobe - multiple	be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	2023-12-15	5.4	Medium
CVE-2023-48615	products	containing the vulnerable field.	2023-12-15	5.4	Medium
<u>CVE-2023-48616</u>	adobe - multiple products	 Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If 	2023-12-15	5.4	Medium
<u>CVE-2023-48617</u>	adobe - multiple products	a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48618</u>	adobe - multiple products	 Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Adobe Experience Manager versions 6.5.18 and earlier are 	2023-12-15	5.4	Medium
<u>CVE-2023-48619</u>	adobe - multiple products	affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
	adaha multinla	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page			
<u>CVE-2023-48620</u>	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field.Adobe Experience Manager versions 6.5.18 and earlier are	2023-12-15	5.4	Medium
CVE-2023-48621	adobe - multiple products	affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	2023-12-15	5.4	Medium

		referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.			
<u>CVE-2023-48622</u>	adobe - multiple products adobe - multiple	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may	2023-12-15	5.4	Medium
CVE-2023-48623	products	be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
<u>CVE-2023-48624</u>	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-12-15	5.4	Medium
	apple - multiple	This issue was addressed through improved state management. This issue is fixed in iOS 17.2 and iPadOS 17.2. Private Browsing			
<u>CVE-2023-42923</u>	products	tabs may be accessed without authentication.	2023-12-12	5.3	Medium
<u>CVE-2023-49058</u>	sap - multiple products	SAP Master Data Governance File Upload application allows an attacker to exploit insufficient validation of path information provided by users, thus characters representing 'traverse to parent directory' are passed through to the file APIs. As a result, it has a low impact to the confidentiality.	2023-12-12	5.3	Medium
	microsoft - office_long_term_s				
<u>CVE-2023-35619</u>	ervicing_channel	Microsoft Outlook for Mac Spoofing Vulnerability	2023-12-12	5.3	Medium
CVE-2023-36012	microsoft - multiple products	DHCP Server Service Information Disclosure Vulnerability	2023-12-12	5.3	Medium
<u>CVE-2023-46713</u>	fortinet - multiple products	An improper output neutralization for logs in Fortinet FortiWeb 6.2.0 - 6.2.8, 6.3.0 - 6.3.23, 7.0.0 - 7.0.9, 7.2.0 - 7.2.5 and 7.4.0 may allow an attacker to forge traffic logs via a crafted URL of the web application. An improper access control vulnerability [CWE-284] in FortiOS	2023-12-12	5.3	Medium
<u>CVE-2023-47536</u>	fortinet - multiple products	version 7.2.0, version 7.0.13 and below, version 6.4.14 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below may allow a remote unauthenticated attacker to bypass the firewall deny geolocalisation policy via timing the bypass with a GeoIP database update. Adobe Experience Manager versions 6.5.18 and earlier are affected by an Improper Access Control vulnerability. An attacker	2023-12-13	5.3	Medium
<u>CVE-2023-48441</u>	adobe - multiple products	could leverage this vulnerability to achieve a low-confidentiality impact within the application. Exploitation of this issue does not require user interaction.	2023-12-15	5.3	Medium
CVE-2023-6839	wso2 - multiple products	Due to improper error handling, a REST API resource could expose a server side error containing an internal WSO2 specific package name in the HTTP response.	2023-12-15	5.3	Medium
	paloaltonetworks -	A credential disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to obtain the plaintext credentials of stored external system integrations such as LDAP, SCP, RADIUS, TACACS+, and SNMP from			
<u>CVE-2023-6791</u>	multiple products	the web interface.	2023-12-13	4.9	Medium
	zoom - multiple	Cryptographic issues Zoom Mobile App for Android, Zoom Mobile App for iOS, and Zoom SDKs for Android and iOS before version 5.16.0 may allow a privileged user to conduct a disclosure of			
CVE-2023-43583	products	information via network access.	2023-12-13	4.9	Medium
<u>CVE-2023-48661</u>	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain an arbitrary file read vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability to read arbitrary files from the target system. In the Streampark platform, when users log in to the system and use certain features, some pages provide a name-based fuzzy search, such as job names, role names, etc. The sql syntax :select * from table where jobName like '%jobName%'. However, the jobName field may receive illegal parameters, leading to SQL injection. This could potentially result in information leakage.	2023-12-14	4.9	Medium
	apache -	Mitigation: Users are recommended to upgrade to version 2.1.2, which fixes			
<u>CVE-2023-30867</u>	streampark	the issue. A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN- OS software enables a malicious authenticated read-write	2023-12-15	4.9	Medium
<u>CVE-2023-6789</u>	paloaltonetworks - multiple products	administrator to store a JavaScript payload using the web interface. Then, when viewed by a properly authenticated	2023-12-13	4.8	Medium

		administrator, the JavaScript payload executes and disguises all associated actions as performed by that unsuspecting authenticated administrator.			
	microsoft - azure_machine_lea				
CVE-2023-35625	rning_software_de velopment_kit	Azure Machine Learning Compute Instance for SDK Users Information Disclosure Vulnerability	2023-12-12	4.7	Medium
	samsung -	A TOCTOU race condition in Samsung Mobile Processor Exynos 9820, Exynos 980, Exynos 1080, Exynos 2100, Exynos 2200, Exynos		,	Wieddam
CVE-2023-42483	exynos_9820_firm ware	1280, and Exynos 1380 can cause unexpected termination of a system.	2023-12-13	4.7	Medium
	samsung -	A race condition issue discovered in Samsung Mobile Processor	2023 12 13		meanan
	exynos_9820_firm	Exynos 9820, 980, 1080, 2100, 2200, 1280, and 1380 allows unintended modifications of values within certain areas.	2022 42 42	47	
<u>CVE-2023-45864</u>	ware	An arbitrary file upload vulnerability in Palo Alto Networks PAN-OS	2023-12-13	4.7	Medium
		software enables an authenticated read-write administrator with			
	paloaltonetworks -	access to the web interface to disrupt system processes and potentially execute arbitrary code with limited privileges on the			
<u>CVE-2023-6794</u>	multiple products	firewall.	2023-12-13	4.7	Medium
		An OS command injection vulnerability in Palo Alto Networks PAN-			
	paloaltonetworks -	OS software enables an authenticated administrator to disrupt system processes and potentially execute arbitrary code with			
<u>CVE-2023-6795</u>	multiple products	limited privileges on the firewall.	2023-12-13	4.7	Medium
	apple - multiple	The issue was addressed with improved checks. This issue is fixed in iOS 17.2 and iPadOS 17.2. An attacker with physical access may			
CVE-2023-42897	products	be able to use Siri to access sensitive user data.	2023-12-12	4.6	Medium
		Workspace ONE Launcher contains a Privilege Escalation			
	vmware - workspace_one_la	Vulnerability. A malicious actor with physical access to Workspace ONE Launcher could utilize the Edge Panel feature to bypass setup			
CVE-2023-34064	uncher	to gain access to sensitive information.	2023-12-12	4.6	Medium
	samsung -	Samsung Mobile Processor and Wearable Processor (Exynos 980,			
CVE-2023-43122	exynos_980_firmw are	850, 1080, 2100, 2200, 1280, 1380, 1330, and W920) allow Information Disclosure in the Bootloader.	2023-12-13	4.6	Medium
<u>CVL 2023 +3122</u>	ure	ONTAP 9 versions 9.12.1P8, 9.13.1P4, and 9.13.1P5 are susceptible	2023 12 13	4.0	Wicdidini
		to a			
		vulnerability which will cause all SAS-attached FIPS 140-2 drives to become unlocked after a system reboot or power cycle or a single			
		SAS-attached FIPS 140-2 drive to become unlocked after			
		reinsertion. This			
	netapp - multiple	could lead to disclosure of sensitive information to an attacker with			
<u>CVE-2023-27317</u>	products	physical access to the unlocked drives.	2023-12-15	4.6	Medium
		SAP Fiori launchpad - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, UI_700 200, SAP_BASIS			
	sap - multiple	793, allows an attacker to use HTTP verb POST on read-only			
CVE-2023-49584	products	service causing low impact on Confidentiality of the application.	2023-12-12	4.3	Medium
		A vulnerability in the AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower			
		Threat Defense (FTD) Software could allow an authenticated,			
		remote attacker to send packets with another VPN user's source IP address. This vulnerability is due to improper validation of the			
		packet's inner source IP address after decryption. An attacker			
		could exploit this vulnerability by sending crafted packets through			
				ļ	
	cisco - multinle	the tunnel. A successful exploit could allow the attacker to send a			
<u>CVE-2023-20275</u>	cisco - multiple products	the tunnel. A successful exploit could allow the attacker to send a packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets.	2023-12-12	4.3	Medium
<u>CVE-2023-20275</u>		packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin	2023-12-12	4.3	Medium
<u>CVE-2023-20275</u>		packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with	2023-12-12	4.3	Medium
<u>CVE-2023-20275</u> <u>CVE-2023-50765</u>		packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID.	2023-12-12 2023-12-13	4.3	Medium
	products	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 			
	products	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to 			
	products	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 			
	products jenkins - scriptler	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. 			
<u>CVE-2023-50765</u>	products jenkins - scriptler jenkins -	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, 	2023-12-13	4.3	Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read 	2023-12-13 2023-12-13	4.3 4.3	Medium
<u>CVE-2023-50765</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. 	2023-12-13	4.3	Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her jenkins -	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read 	2023-12-13 2023-12-13	4.3 4.3	Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her jenkins - dingding_json_pus her	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier does not mask access tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them. 	2023-12-13 2023-12-13	4.3 4.3	Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u> <u>CVE-2023-50772</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her jenkins - dingding_json_pus her jenkins -	packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier does not mask access tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them. A cross-site request forgery (CSRF) vulnerability in Jenkins	2023-12-13 2023-12-13 2023-12-13	4.3 4.3 4.3	Medium Medium Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u> <u>CVE-2023-50772</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her jenkins - dingding_json_pus her	 packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier does not mask access tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them. 	2023-12-13 2023-12-13 2023-12-13	4.3 4.3 4.3	Medium Medium Medium
<u>CVE-2023-50765</u> <u>CVE-2023-50769</u> <u>CVE-2023-50772</u> <u>CVE-2023-50773</u>	products jenkins - scriptler jenkins - nexus_platform jenkins - dingding_json_pus her jenkins - dingding_json_pus her jenkins - dingding_json_pus her jenkins -	packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets. A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID. Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0- 03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. Jenkins Dingding JSON Pusher Plugin 2.0 and earlier does not mask access tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them. A cross-site request forgery (CSRF) vulnerability in Jenkins Deployment Dashboard Plugin 1.0.10 and earlier allows attackers	2023-12-13 2023-12-13 2023-12-13 2023-12-13	4.3 4.3 4.3	Medium Medium Medium

		Item/Extended Read permission or access to the Jenkins controller			
		file system.			
		Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier does not mask			
		PaaSLane authentication tokens displayed on the job configuration			
	jenkins -	form, increasing the potential for attackers to observe and capture			
CVE-2023-50777	paaslane estimate	them.	2023-12-13	4.3	Medium
<u>CVL 2023 30777</u>		Missing permission checks in Jenkins PaaSLane Estimate Plugin			
		1.0.4 and earlier allow attackers with Overall/Read permission to			
	jenkins -	connect to an attacker-specified URL using an attacker-specified			
CVE-2023-50779	paaslane_estimate	token.	2023-12-13	4.3	Medium
<u>CVL 2023 30775</u>	padolarie_contrace	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-	2020 12 10		mearan
		VED and 3957-VEC could allow a remote authenticated user to			
		obtain sensitive information, caused by improper filtering of URLs.			
	ibm -	By submitting a specially crafted HTTP GET request, an attacker			
	virtualization_engin	could exploit this vulnerability to view application source code,			
	e_ts7760_3957-	system configuration information, or other sensitive data related			
CVE-2023-49877	vec firmware	to the Management Interface. IBM X-Force ID: 272651.	2023-12-13	4.3	Medium
<u>UVL-2023-49011</u>	vec_innware	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-	2023-12-13	4.5	weululli
	ibm	VED and 3957-VEC could allow a remote attacker to obtain			
	ibm -				
	virtualization_engin	sensitive information when a detailed technical error message is			
CVF 2022 40070	e_ts7760_3957-	returned in the browser. This information could be used in further	2022 42 42	4.2	
<u>CVE-2023-49878</u>	vec_firmware	attacks against the system. IBM X-Force ID: 272652.	2023-12-13	4.3	Medium
	microsoft -	Microsoft Edge (Chromium-based) Security Feature Bypass			
<u>CVE-2023-36878</u>	edge_chromium	Vulnerability	2023-12-15	4.3	Medium
		SAP Cloud Connector - version 2.0, allows an authenticated user			
		with low privilege to perform Denial of service attack from			
		adjacent UI by sending a malicious request which leads to low			
	sap -	impact on the availability and no impact on confidentiality or			
<u>CVE-2023-49578</u>	cloud_connector	Integrity of the application.	2023-12-12	3.5	Low
		Adobe Experience Manager versions 6.5.18 and earlier are			
		affected by an Improper Input Validation vulnerability. A low-			
		privileged attacker could leverage this vulnerability to achieve a			
	adobe - multiple	low-integrity impact within the application. Exploitation of this			
<u>CVE-2023-48608</u>	products	issue requires user interaction.	2023-12-15	3.5	Low
		A vulnerability has been identified in SINEC INS (All versions < V1.0			
		SP2 Update 2). The Web UI of affected devices does not check the			
		length of parameters in certain conditions. This allows a malicious			
	siemens - multiple	admin to crash the server by sending a crafted request to the			
<u>CVE-2023-48429</u>	products	server. The server will automatically restart.	2023-12-12	2.7	Low
		A vulnerability has been identified in SINEC INS (All versions < V1.0			
		SP2 Update 2). The REST API of affected devices does not check			
		the length of parameters in certain conditions. This allows a			
	siemens - multiple	malicious admin to crash the server by sending a crafted request			
CVE-2023-48430	products	to the API. The server will automatically restart.	2023-12-12	2.7	Low
		An improper privilege management vulnerability in Palo Alto			
		Networks PAN-OS software enables an authenticated read-only			
	paloaltonetworks -	administrator to revoke active XML API keys from the firewall and			
CVE-2023-6793	multiple products	disrupt XML API usage.	2023-12-13	2.7	Low
		This issue was addressed with improved state management. This			
		issue is fixed in macOS Sonoma 14.2. Secure text fields may be			
		displayed via the Accessibility Keyboard when using a physical			
CVE-2023-42874	apple - macos	keyboard.	2023-12-12	2.4	Low
3.2 2020 12071		-,		··	

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. In addition, it is the entity's or individual's الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة. responsibility to ensure the implementation of appropriate recommendations.