تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 10 ديسمبر إلى 17 ديسمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـ CVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـ CVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـ CVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 10th of December to 17th of December. Vulnerabilities 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-48417	google - chromecast_firmware	Missing Permission checks resulting in unauthorized access and Manipulation in KeyChainActivity Application	2023-12-11	9.8	Critical
CVE-2023-48424	google - chromecast_firmware	U-Boot shell vulnerability resulting in Privilege escalation in a production device	2023-12-11	9.8	Critical
CVE-2023-48425	google - chromecast_firmware	U-Boot vulnerability resulting in persistent Code Execution	2023-12-11	9.8	Critical
CVE-2023-6181	google - chromecast_firmware	An oversight in BCB handling of reboot reason that allows for persistent code execution	2023-12-11	9.8	Critical
CVE-2023-49583	sap - \@sap\/xssec	SAP BTP Security Services Integration Library ([Node.js] @sap/xssec - versions < 3.6.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	2023-12-12	9.8	Critical
CVE-2023-50422	sap - multiple products	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 unauthenticated attacker can obtain arbitrary permissions within the application.	2023-12-12	9.8	Critical
CVE-2023-50423	sap - sap-xssec	SAP BTP Security Services Integration Library ([Python] sap-xssec) - versions < 4.1.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	2023-12-12	9.8	Critical
CVE-2023-50424	sap - cloud-security-client-go	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 exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	2023-12-12	9.8	Critical
CVE-2023-48427	siemens - multiple products	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 as well as to manipulate responses, potentially allowing an attacker to escalate privileges.	2023-12-12	9.8	Critical
CVE-2023-48084	nagios - nagios_xi	Nagios XI before version 5.11.3 was discovered to contain a SQL injection vulnerability via the bulk modification tool.	2023-12-14	9.8	Critical
CVE-2023-48085	nagios - nagios_xi	Nagios XI before version 5.11.3 was discovered to contain a remote code execution (RCE) vulnerability via the component command_test.php.	2023-12-14	9.8	Critical
CVE-2023-29234	apache - multiple products	A deserialization vulnerability existed when decode a malicious package.This issue affects Apache Dubbo: from 3.1.0 through 3.1.10, from 3.2.0 through 3.2.4.	2023-12-15	9.8	Critical

		Users are recommended to upgrade to the latest version, which fixes the issue.			
CVE-2023-46279	apache - dubbo	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 fixes the issue.	2023-12-15	9.8	Critical
CVE-2023-50089	netgear - wnr2000_firmware	A Command Injection vulnerability exists in NETGEAR WNR2000v4 version 1.0.0.70. When using HTTP for SOAP authentication, command execution occurs during the process after successful authentication.	2023-12-15	9.8	Critical
CVE-2023-49581	sap - multiple products	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 a database table. By doing so the attacker could increase response times of the AS ABAP, leading to mild impact on availability.	2023-12-12	9.4	Critical
CVE-2023-42890	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, macOS Sonoma 14.2, watchOS 10.2, iOS 17.2 and iPadOS 17.2, tvOS 17.2. Processing web content may lead to arbitrary code execution.	2023-12-12	8.8	High
CVE-2023-42910	apple - macos	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 termination or arbitrary code execution.	2023-12-12	8.8	High
CVE-2023-46281	siemens - multiple products	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) 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). When accessing the UMC Web-UI from affected products, UMC uses an overly permissive CORS policy. This could allow an attacker to trick a legitimate user to trigger unwanted behavior.	2023-12-12	8.8	High
CVE-2023-35630	microsoft - multiple products	Internet Connection Sharing (ICS) Remote Code Execution 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
CVE-2023-35639	microsoft - multiple products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2023-12-12	8.8	High
CVE-2023-35641	microsoft - multiple products	Internet Connection Sharing (ICS) Remote Code Execution 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
CVE-2022-27488	fortinet - multiple products	A cross-site request forgery (CSRF) in Fortinet FortiVoiceEnterprise 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 commands on the CLI via tricking an authenticated administrator to execute malicious GET requests.	2023-12-13	8.8	High
CVE-2023-36639	fortinet - multiple products	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 unauthorized code or commands via specially crafted API requests.	2023-12-13	8.8	High
CVE-2023-41678	fortinet - multiple products	A double free in Fortinet FortiOS versions 7.0.0 through 7.0.5, FortiPAM version 1.0.0 through 1.0.3, 1.1.0 through 1.1.1 allows attacker to execute unauthorized code or commands via specifically crafted request.	2023-12-13	8.8	High
CVE-2023-48782	fortinet - fortiwlm	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 or commands via specifically crafted http get request parameters	2023-12-13	8.8	High
CVE-2023-48791	fortinet - multiple products	An improper neutralization of special elements used in a command ('Command Injection') vulnerability [CWE-77] in FortiPortal version 7.2.0, version 7.0.6 and below may allow a remote authenticated attacker with at least R/W permission to execute unauthorized commands via specifically crafted arguments in the Schedule System Backup page field.	2023-12-13	8.8	High
CVE-2023-44251	fortinet - multiple products	** UNSUPPORTED WHEN ASSIGNED **A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in Fortinet FortiWAN version 5.2.0 through 5.2.1 and	2023-12-13	8.8	High

		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.			
CVE-2023-44252	fortinet - multiple products	** 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 authenticated attacker to escalate his privileges via HTTP or HTTPs requests with crafted JWT token values.	2023-12-13	8.8	High
CVE-2023-50766	jenkins - nexus_platform	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allows attackers to send an HTTP request to an attacker-specified URL and parse the response as XML.	2023-12-13	8.8	High
CVE-2023-50768	jenkins - nexus_platform	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-12-13	8.8	High
CVE-2023-50778	jenkins - paaslane_estimate	A cross-site request forgery (CSRF) vulnerability in Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier allows attackers to connect to an attacker-specified URL using an attacker-specified token.	2023-12-13	8.8	High
CVE-2023-43586	zoom - multiple products	Path traversal in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows may allow an authenticated user to conduct an escalation of privilege via network access.	2023-12-13	8.8	High
CVE-2023-45185	ibm - multiple products	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 could allow an attacker to execute remote code. Due to improper authority checks the attacker could perform operations on the PC under the user's authority. IBM X-Force ID: 268273.	2023-12-14	8.8	High
CVE-2023-6702	google - chrome	Type confusion in V8 in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
CVE-2023-6703	google - chrome	Use after free in Blink in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
CVE-2023-6704	google - chrome	Use after free in libavif in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted image file. (Chromium security severity: High)	2023-12-14	8.8	High
CVE-2023-6705	google - chrome	Use after free in WebRTC in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
CVE-2023-6706	google - chrome	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 crafted HTML page. (Chromium security severity: High)	2023-12-14	8.8	High
CVE-2023-6707	google - chrome	Use after free in CSS in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-12-14	8.8	High
CVE-2023-48431	siemens - multiple products	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 malicious UMC server or by manipulating the traffic from a legitimate UMC server (i.e. leveraging CVE-2023-48427).	2023-12-12	8.6	High
CVE-2023-42481	sap - commerce_cloud	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 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.	2023-12-12	8.1	High
CVE-2023-35628	microsoft - multiple products	Windows MSHTML Platform Remote Code Execution Vulnerability	2023-12-12	8.1	High
CVE-2023-36005	microsoft - multiple products	Windows Telephony Server Elevation of Privilege Vulnerability	2023-12-12	8.1	High
CVE-2023-50764	jenkins - scriptler	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.	2023-12-13	8.1	High
CVE-2023-50774	jenkins - multiple products	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.	2023-12-13	8.1	High
CVE-2023-40446	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing maliciously crafted input may lead to arbitrary code execution in user-installed apps.	2023-12-12	7.8	High

CVE-2023-42882	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing an image may lead to arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42886	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. A user may be able to cause unexpected app termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42899	apple - multiple products	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. Processing an image may lead to arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42901	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42902	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42903	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42904	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42905	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42906	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42907	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42908	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42909	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42911	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42912	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-42926	apple - macos	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 termination or arbitrary code execution.	2023-12-12	7.8	High
CVE-2023-21740	microsoft - multiple products	Windows Media Remote Code Execution Vulnerability	2023-12-12	7.8	High
CVE-2023-35631	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-35632	microsoft - multiple products	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-35633	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-35644	microsoft - multiple products	Windows Sysmain Service Elevation of Privilege	2023-12-12	7.8	High
CVE-2023-36011	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-36391	microsoft - windows_11_23h2	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-36696	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-12-12	7.8	High
CVE-2023-5764	redhat - multiple products	A template injection flaw was found in Ansible where a user's controller internal templating operations may remove the unsafe designation from template data. This issue could allow an attacker	2023-12-12	7.8	High

		to use a specially crafted file to introduce code injection when supplying templating data.			
CVE-2023-40716	fortinet - multiple products	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 attacker to execute unauthorized commands via specifically crafted arguments when running execute restore/backup .	2023-12-13	7.8	High
CVE-2023-6377	redhat - enterprise_linux_eus	A flaw was found in xorg-server. Querying or changing XKB button actions such as moving from a touchpad to a mouse can result in out-of-bounds memory reads and writes. This may allow local privilege escalation or possible remote code execution in cases where X11 forwarding is involved.	2023-12-13	7.8	High
CVE-2022-22942	vmware - multiple products	The vmwgfx driver contains a local privilege escalation vulnerability that allows unprivileged users to gain access to files opened by other processes on the system through a dangling 'file' pointer.	2023-12-13	7.8	High
CVE-2023-47063	adobe - multiple products	Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-47074	adobe - multiple products	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 vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-47075	adobe - multiple products	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. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48625	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48626	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48627	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48628	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48629	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48630	adobe - substance_3d_sampler	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48632	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 write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48633	adobe - multiple products	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-48634	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High

CVE-2023-48639	adobe - substance_3d_designer	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	7.8	High
CVE-2023-45166	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the piodmgrsu command to obtain elevated privileges. IBM X-Force ID: 267964.	2023-12-13	7.8	High
CVE-2023-45170	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the piobe command to escalate privileges or cause a denial of service. IBM X-Force ID: 267968.	2023-12-13	7.8	High
CVE-2023-45174	ibm - multiple products	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 privileges or cause a denial of service. IBM X-Force ID: 267972.	2023-12-13	7.8	High
CVE-2023-41720	ivanti - multiple products	A vulnerability exists on all versions of Ivanti Connect Secure 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 allows the attacker to gain elevated execution privileges on the affected system.	2023-12-14	7.8	High
CVE-2023-42478	sap - multiple products	SAP Business Objects Business Intelligence Platform is vulnerable to stored XSS allowing an attacker to upload agnostic documents in the system which when opened by any other user could lead to high impact on integrity of the application.	2023-12-12	7.6	High
CVE-2022-48616	huawei - ar617vw_firmware	A Huawei data communication product has a command injection vulnerability. Successful exploitation of this vulnerability may allow attackers to gain higher privileges.	2023-12-12	7.5	High
CVE-2022-47374	siemens - 6es7412-2ek07-0ab0_firmware	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. This could allow an attacker to exhaust system resources and create a denial of service condition for the device.	2023-12-12	7.5	High
CVE-2022-47375	siemens - 6es7412-2ek07-0ab0_firmware	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. This could allow an attacker to create a buffer overflow and create a denial of service condition for the device.	2023-12-12	7.5	High
CVE-2023-38380	siemens - 6gk7243-8rx30-0xe0_firmware	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
CVE-2023-46156	siemens - simatic_drive_controller_cpu_1504d_tf_firmware	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 restart is needed to restore normal operations.	2023-12-12	7.5	High

CVE-2023-46283	siemens - multiple products	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) 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). The affected application contains an out of bounds write past the end of an allocated buffer when handling specific requests on port 4002/tcp. This could allow an attacker to crash the application. The corresponding service is auto-restarted after the crash.	2023-12-12	7.5	High
CVE-2023-46284	siemens - multiple products	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) 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). 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. This could allow an attacker to crash the application. The corresponding service is auto-restarted after the crash.	2023-12-12	7.5	High
CVE-2023-46285	siemens - multiple products	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) 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). 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 corresponding service is auto-restarted after the crash is detected by a watchdog.	2023-12-12	7.5	High
CVE-2023-35621	microsoft - multiple products	Microsoft Dynamics 365 Finance and Operations Denial of Service Vulnerability	2023-12-12	7.5	High
CVE-2023-35622	microsoft - multiple products	Windows DNS Spoofing Vulnerability	2023-12-12	7.5	High
CVE-2023-35638	microsoft - multiple products	DHCP Server Service Denial of Service Vulnerability	2023-12-12	7.5	High
CVE-2023-35643	microsoft - multiple products	DHCP Server Service Information Disclosure Vulnerability	2023-12-12	7.5	High
CVE-2023-36004	microsoft - multiple products	Windows DPAPI (Data Protection Application Programming Interface) Spoofing Vulnerability	2023-12-12	7.5	High
CVE-2023-36010	microsoft - malware_protection_platform	Microsoft Defender Denial of Service Vulnerability	2023-12-12	7.5	High
CVE-2023-5379	redhat - multiple products	A flaw was found in Undertow. When an AJP request is sent that 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 allow a malicious user could to repeatedly send requests that exceed the max-header-size, causing a Denial of Service (DoS).	2023-12-12	7.5	High
CVE-2022-43843	ibm - multiple products	IBM Spectrum Scale 5.1.5.0 through 5.1.5.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 239080.	2023-12-14	7.5	High
CVE-2023-43042	ibm - storage_virtualize	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and IBM Storage Virtualize 8.3 products use default passwords for a privileged user. IBM X-Force ID: 266874.	2023-12-14	7.5	High
CVE-2023-45184	ibm - multiple products	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 could allow an attacker to obtain a decryption key due to improper authority checks. IBM X-Force ID: 268270.	2023-12-14	7.5	High
CVE-2023-48631	adobe - css-tools	@adobe/css-tools versions 4.3.1 and earlier are affected by an Improper Input Validation vulnerability that could result in a denial of service while attempting to parse CSS.	2023-12-14	7.5	High
CVE-2023-48660	dell - multiple products	Dell vApp Manger, versions prior to 9.2.4.x contain an arbitrary file read vulnerability. A remote attacker could potentially exploit this vulnerability to read arbitrary files from the target system.	2023-12-14	7.5	High

CVE-2023-48671	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain an information disclosure vulnerability. A remote attacker could potentially exploit this vulnerability leading to obtain sensitive information that may aid in further attacks.	2023-12-14	7.5	High
CVE-2023-4694	hp - officejet_pro_8730_d9l19a_firmware	Certain HP OfficeJet Pro printers are potentially vulnerable to a Denial of Service when sending a SOAP message to the service on TCP port 3911 that contains a body but no header.	2023-12-14	7.5	High
CVE-2023-6836	wso2 - api_manager	Multiple WSO2 products have been identified as vulnerable due to an XML External Entity (XXE) attack abuses a widely available but rarely used feature of XML parsers to access sensitive information.	2023-12-15	7.5	High
CVE-2023-39340	ivanti - multiple products	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance.	2023-12-16	7.5	High
CVE-2023-36019	microsoft - multiple products	Microsoft Power Platform Connector Spoofing Vulnerability	2023-12-12	7.4	High
CVE-2023-49580	sap - multiple products	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 impact on integrity and availability, e.g. also increasing the response times of the AS ABAP.	2023-12-12	7.3	High
CVE-2023-35624	microsoft - azure_connected_machine_agent	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2023-12-12	7.3	High
CVE-2023-36003	microsoft - multiple products	XAML Diagnostics Elevation of Privilege Vulnerability	2023-12-12	7.3	High
CVE-2023-48428	siemens - multiple products	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 denial-of-service condition or potentially issue commands on system level.	2023-12-12	7.2	High
CVE-2023-41719	ivanti - multiple products	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution.	2023-12-14	7.2	High
CVE-2023-48662	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
CVE-2023-48663	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
CVE-2023-48664	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
CVE-2023-48665	dell - multiple products	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	2023-12-14	7.2	High
CVE-2023-6542	sap - emarsys_sdk	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 links on the device.	2023-12-12	7.1	High
CVE-2022-48615	huawei - ar617vw_firmware	An improper access control vulnerability exists in a Huawei datacom product. Attackers can exploit this vulnerability to obtain partial device information.	2023-12-12	7.1	High
CVE-2023-6407	schneider-electric - easy_ups_online_monitoring_software	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.	2023-12-14	7.1	High
CVE-2023-42476	sap - businessobjects_web_intelligence	SAP Business Objects Web Intelligence - version 420, allows an authenticated attacker to inject JavaScript code into Web Intelligence documents which is then executed in the victim's browser each time the vulnerable page is visited. Successful exploitation can lead to exposure of the data that the user has	2023-12-12	6.8	Medium

		access to. In the worst case, attacker could access data from reporting databases.			
CVE-2022-42784	siemens - 6ed1052-1md08-0ba1_firmware	A vulnerability has been identified in LOGO! 12/24RCE (All versions >= V8.3), LOGO! 12/24RCEo (All versions >= V8.3), LOGO! 230RCE (All versions >= V8.3), LOGO! 230RCEo (All versions >= V8.3), LOGO! 24CE (All versions >= V8.3), LOGO! 24CEo (All versions >= V8.3), LOGO! 24RCE (All versions >= V8.3), LOGO! 24RCEo (All versions >= V8.3), SIPLUS LOGO! 12/24RCE (All versions >= V8.3), SIPLUS LOGO! 12/24RCEo (All versions >= V8.3), SIPLUS LOGO! 230RCE (All versions >= V8.3), SIPLUS LOGO! 230RCEo (All versions >= V8.3), SIPLUS LOGO! 24CE (All versions >= V8.3), SIPLUS LOGO! 24CEo (All versions >= V8.3), SIPLUS LOGO! 24RCE (All versions >= V8.3), SIPLUS LOGO! 24RCEo (All 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-2023-35629	microsoft - multiple products	Microsoft USBHUB 3.0 Device Driver Remote Code Execution Vulnerability	2023-12-12	6.8	Medium
CVE-2023-49691	siemens - 6gk6108-4am00-2ba2_firmware	A 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 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 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 (EVDO) (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 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). 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
CVE-2023-49692	siemens - 6gk6108-4am00-2ba2_firmware	A 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 < 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 S615 (All 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 the IPSEC configuration. This could allow malicious local administrators to issue commands on system level after a new connection is established.	2023-12-12	6.7	Medium
CVE-2023-50770	jenkins - openid	Jenkins OpenId Connect Authentication Plugin 2.6 and earlier stores a password of a local user account used as an anti-lockout 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
CVE-2023-4421	mozilla - nss	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 issue was fixed by implementing the implicit rejection algorithm, in	2023-12-12	6.5	Medium

		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.			
CVE-2023-35636	microsoft - multiple products	Microsoft Outlook Information Disclosure Vulnerability	2023-12-12	6.5	Medium
CVE-2023-35642	microsoft - multiple products	Internet Connection Sharing (ICS) Denial of Service Vulnerability	2023-12-12	6.5	Medium
CVE-2023-43585	zoom - multiple products	Improper access control in Zoom Mobile App for iOS and Zoom SDKs for iOS before version 5.16.5 may allow an authenticated user to conduct a disclosure of information via network access.	2023-12-13	6.5	Medium
CVE-2023-49646	zoom - multiple products	Improper authentication in some Zoom clients before version 5.16.5 may allow an authenticated user to conduct a denial of service via network access.	2023-12-13	6.5	Medium
CVE-2023-21751	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-12-14	6.5	Medium
CVE-2023-45182	ibm - multiple products	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 password, a local attacker could exploit this vulnerability to obtain the password to other systems. IBM X-Force ID: 268265.	2023-12-14	6.5	Medium
CVE-2023-49587	sap - solution_manager	SAP Solution Manager - version 720, allows an authorized attacker 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	Medium
CVE-2023-42914	apple - multiple products	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 break out of its sandbox.	2023-12-12	6.3	Medium
CVE-2023-6792	paloaltonetworks - multiple products	An OS command injection vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated API user to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	2023-12-13	6.3	Medium
CVE-2023-42479	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	Medium
CVE-2023-49577	sap - multiple products	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 of the application.	2023-12-12	6.1	Medium
CVE-2023-4958	redhat - multiple products	In Red Hat Advanced Cluster Security (RHACS), it was found that 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 other actions.	2023-12-12	6.1	Medium
CVE-2023-46282	siemens - multiple products	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) 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 another (possibly privileged) user.	2023-12-12	6.1	Medium
CVE-2023-50771	jenkins - openid	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 phishing attacks.	2023-12-13	6.1	Medium
CVE-2023-6790	paloaltonetworks - multiple products	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 when they view a specifically crafted link to the PAN-OS web interface.	2023-12-13	6.1	Medium
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	Medium

CVE-2023-6838	wso2 - multiple products	Reflected XSS vulnerability can be exploited by tampering a request parameter in Authentication Endpoint. This can be performed in both authenticated and unauthenticated requests.	2023-12-15	6.1	Medium
CVE-2023-45725	apache - couchdb	Design document functions which receive a user http request object may expose authorization or session cookie headers of the user who accesses the document. 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. 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
CVE-2023-6679	linux - linux_kernel	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. This issue could be exploited to trigger a denial of service.	2023-12-11	5.5	Medium
CVE-2023-42883	apple - multiple products	The issue was addressed with improved memory handling. This 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
CVE-2023-42884	apple - multiple products	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, tvOS 17.2, iOS 16.7.3 and iPadOS 16.7.3. An app may be able to disclose kernel memory.	2023-12-12	5.5	Medium
CVE-2023-42891	apple - multiple products	An authentication issue was addressed with improved state 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 monitor keystrokes without user permission.	2023-12-12	5.5	Medium
CVE-2023-42894	apple - multiple products	This issue was addressed with improved redaction of sensitive 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
CVE-2023-42898	apple - multiple products	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 code execution.	2023-12-12	5.5	Medium
CVE-2023-42900	apple - macos	The issue was addressed with improved checks. This issue is fixed 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 products	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 may be able to access sensitive user data.	2023-12-12	5.5	Medium
CVE-2023-42922	apple - multiple products	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 16.7.3, macOS Monterey 12.7.2. An app may be able to read sensitive location information.	2023-12-12	5.5	Medium
CVE-2023-42924	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.	2023-12-12	5.5	Medium
CVE-2023-42932	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, macOS Monterey 12.7.2. An app may be able to access protected user data.	2023-12-12	5.5	Medium
CVE-2022-46141	siemens - simatic_step_7	A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) (All versions < V19). An information disclosure vulnerability could 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 application.	2023-12-12	5.5	Medium
CVE-2023-35635	microsoft - multiple products	Windows Kernel Denial of Service Vulnerability	2023-12-12	5.5	Medium
CVE-2023-36009	microsoft - multiple products	Microsoft Word Information Disclosure Vulnerability	2023-12-12	5.5	Medium

CVE-2023-47076	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-47077	adobe - multiple products	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 victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-44362	adobe - prelude	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 file.	2023-12-13	5.5	Medium
CVE-2023-47061	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.	2023-12-13	5.5	Medium
CVE-2023-47062	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.	2023-12-13	5.5	Medium
CVE-2023-47078	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.	2023-12-13	5.5	Medium
CVE-2023-47079	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.	2023-12-13	5.5	Medium
CVE-2023-47080	adobe - substance_3d_stager	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_stager	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
CVE-2023-48636	adobe - substance_3d_designer	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 that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-48637	adobe - substance_3d_designer	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 that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-48638	adobe - substance_3d_designer	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 that a victim must open a malicious file.	2023-12-13	5.5	Medium
CVE-2023-36020	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting 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.			
CVE-2023-41844	fortinet - multiple products	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 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 crafted HTTP requests in capture traffic endpoint.	2023-12-13	5.4	Medium
CVE-2023-45587	fortinet - multiple products	An 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 through 3.2.4 and 3.1.0 through 3.1.5 allows attacker to execute unauthorized code or commands via crafted HTTP requests	2023-12-13	5.4	Medium
CVE-2023-50767	jenkins - nexus_platform	Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML.	2023-12-13	5.4	Medium
CVE-2023-6134	redhat - single_sign-on	A flaw was found in Keycloak that prevents certain schemes in redirects, but permits them if a wildcard is appended to the token. This issue could allow an attacker to submit a specially crafted request leading to cross-site scripting (XSS) or further attacks. This flaw is the result of an incomplete fix for CVE-2020-10748.	2023-12-14	5.4	Medium
CVE-2023-47064	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
CVE-2023-47065	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
CVE-2023-48440	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
CVE-2023-48442	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
CVE-2023-48443	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48444	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
CVE-2023-48445	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
CVE-2023-48446	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
CVE-2023-48447	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48448	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48449	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	2023-12-15	5.4	Medium

		referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.			
CVE-2023-48450	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
CVE-2023-48451	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
CVE-2023-48452	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
CVE-2023-48453	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
CVE-2023-48454	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
CVE-2023-48455	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48456	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
CVE-2023-48457	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
CVE-2023-48458	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
CVE-2023-48459	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
CVE-2023-48460	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
CVE-2023-48461	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
CVE-2023-48462	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
CVE-2023-48463	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
CVE-2023-48464	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
CVE-2023-48465	adobe - multiple products	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

		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.			
CVE-2023-48466	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
CVE-2023-48467	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
CVE-2023-48468	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
CVE-2023-48469	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
CVE-2023-48470	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
CVE-2023-48471	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
CVE-2023-48472	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
CVE-2023-48473	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
CVE-2023-48474	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
CVE-2023-48475	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
CVE-2023-48476	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
CVE-2023-48477	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
CVE-2023-48478	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
CVE-2023-48479	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
CVE-2023-48480	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

CVE-2023-48481	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
CVE-2023-48482	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
CVE-2023-48483	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
CVE-2023-48484	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
CVE-2023-48485	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
CVE-2023-48486	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
CVE-2023-48487	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
CVE-2023-48488	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
CVE-2023-48489	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
CVE-2023-48490	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
CVE-2023-48491	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
CVE-2023-48492	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
CVE-2023-48493	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
CVE-2023-48494	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
CVE-2023-48495	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
CVE-2023-48496	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	2023-12-15	5.4	Medium

		referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.			
CVE-2023-48497	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48498	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48499	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48500	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48501	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
CVE-2023-48502	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
CVE-2023-48503	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
CVE-2023-48504	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
CVE-2023-48505	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
CVE-2023-48506	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
CVE-2023-48507	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
CVE-2023-48508	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
CVE-2023-48509	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
CVE-2023-48510	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

CVE-2023-48511	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
CVE-2023-48512	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
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	Medium
CVE-2023-48514	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
CVE-2023-48515	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
CVE-2023-48516	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
CVE-2023-48517	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
CVE-2023-48518	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
CVE-2023-48519	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
CVE-2023-48520	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
CVE-2023-48521	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
CVE-2023-48522	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
CVE-2023-48523	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

CVE-2023-48524	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
CVE-2023-48525	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
CVE-2023-48526	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48527	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
CVE-2023-48528	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
CVE-2023-48529	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
CVE-2023-48530	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
CVE-2023-48531	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
CVE-2023-48532	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
CVE-2023-48533	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
CVE-2023-48534	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
CVE-2023-48535	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
CVE-2023-48536	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
CVE-2023-48537	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

CVE-2023-48538	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
CVE-2023-48539	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
CVE-2023-48540	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
CVE-2023-48541	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
CVE-2023-48542	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
CVE-2023-48543	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
CVE-2023-48544	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
CVE-2023-48545	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
CVE-2023-48546	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
CVE-2023-48547	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
CVE-2023-48548	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
CVE-2023-48549	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
CVE-2023-48550	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
CVE-2023-48551	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	Medium

		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.			
CVE-2023-48552	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
CVE-2023-48553	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
CVE-2023-48554	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
CVE-2023-48555	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
CVE-2023-48556	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
CVE-2023-48557	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
CVE-2023-48558	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
CVE-2023-48559	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
CVE-2023-48560	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
CVE-2023-48561	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
CVE-2023-48562	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
CVE-2023-48563	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
CVE-2023-48564	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	2023-12-15	5.4	Medium

		executed in a victim’s browser when they browse to the page containing the vulnerable field.			
CVE-2023-48565	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
CVE-2023-48566	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
CVE-2023-48567	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
CVE-2023-48568	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
CVE-2023-48569	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
CVE-2023-48570	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
CVE-2023-48571	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
CVE-2023-48572	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
CVE-2023-48573	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
CVE-2023-48574	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
CVE-2023-48575	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
CVE-2023-48576	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
CVE-2023-48577	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
CVE-2023-48578	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	Medium

		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.			
CVE-2023-48579	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
CVE-2023-48580	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
CVE-2023-48581	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
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	Medium
CVE-2023-48583	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
CVE-2023-48584	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
CVE-2023-48585	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
CVE-2023-48586	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
CVE-2023-48587	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
CVE-2023-48588	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
CVE-2023-48589	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
CVE-2023-48590	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
CVE-2023-48591	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
CVE-2023-48592	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	Medium

		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.			
CVE-2023-48593	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
CVE-2023-48594	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
CVE-2023-48595	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
CVE-2023-48596	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
CVE-2023-48597	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
CVE-2023-48598	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
CVE-2023-48599	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
CVE-2023-48600	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
CVE-2023-48601	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48602	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
CVE-2023-48603	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
CVE-2023-48604	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
CVE-2023-48605	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

CVE-2023-48606	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
CVE-2023-48607	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48609	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
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
CVE-2023-48611	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
CVE-2023-48612	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
CVE-2023-48613	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
CVE-2023-48614	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
CVE-2023-48615	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
CVE-2023-48616	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
CVE-2023-48617	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
CVE-2023-48618	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
CVE-2023-48619	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
CVE-2023-48620	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
CVE-2023-48621	adobe - multiple products	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	2023-12-15	5.4	Medium

		referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.			
CVE-2023-48622	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
CVE-2023-48623	adobe - multiple products	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 be executed within the context of the victim's browser.	2023-12-15	5.4	Medium
CVE-2023-48624	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
CVE-2023-42923	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 17.2 and iPadOS 17.2. Private Browsing tabs may be accessed without authentication.	2023-12-12	5.3	Medium
CVE-2023-49058	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
CVE-2023-35619	microsoft - office_long_term_servicing_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
CVE-2023-46713	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.	2023-12-13	5.3	Medium
CVE-2023-47536	fortinet - multiple products	An improper access control vulnerability [CWE-284] in FortiOS 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.	2023-12-13	5.3	Medium
CVE-2023-48441	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by an Improper Access Control vulnerability. An attacker 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
CVE-2023-6791	paloaltonetworks - multiple products	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 the web interface.	2023-12-13	4.9	Medium
CVE-2023-43583	zoom - multiple products	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 information via network access.	2023-12-13	4.9	Medium
CVE-2023-48661	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.	2023-12-14	4.9	Medium
CVE-2023-30867	apache - streampark	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. Mitigation: Users are recommended to upgrade to version 2.1.2, which fixes the issue.	2023-12-15	4.9	Medium
CVE-2023-6789	paloaltonetworks - multiple products	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a malicious authenticated read-write 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.			
CVE-2023-35625	microsoft - azure_machine_learning_software_development_kit	Azure Machine Learning Compute Instance for SDK Users Information Disclosure Vulnerability	2023-12-12	4.7	Medium
CVE-2023-42483	samsung - exynos_9820_firmware	A TOCTOU race condition in Samsung Mobile Processor Exynos 9820, Exynos 980, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, and Exynos 1380 can cause unexpected termination of a system.	2023-12-13	4.7	Medium
CVE-2023-45864	samsung - exynos_9820_firmware	A race condition issue discovered in Samsung Mobile Processor Exynos 9820, 980, 1080, 2100, 2200, 1280, and 1380 allows unintended modifications of values within certain areas.	2023-12-13	4.7	Medium
CVE-2023-6794	paloaltonetworks - multiple products	An arbitrary file upload vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write administrator with access to the web interface to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	2023-12-13	4.7	Medium
CVE-2023-6795	paloaltonetworks - multiple products	An OS command injection vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	2023-12-13	4.7	Medium
CVE-2023-42897	apple - multiple products	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 be able to use Siri to access sensitive user data.	2023-12-12	4.6	Medium
CVE-2023-34064	vmware - workspace_one_launcher	Workspace ONE Launcher contains a Privilege Escalation Vulnerability. A malicious actor with physical access to Workspace ONE Launcher could utilize the Edge Panel feature to bypass setup to gain access to sensitive information.	2023-12-12	4.6	Medium
CVE-2023-43122	samsung - exynos_980_firmware	Samsung Mobile Processor and Wearable Processor (Exynos 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, and W920) allow Information Disclosure in the Bootloader.	2023-12-13	4.6	Medium
CVE-2023-27317	netapp - multiple products	ONTAP 9 versions 9.12.1P8, 9.13.1P4, and 9.13.1P5 are susceptible 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 could lead to disclosure of sensitive information to an attacker with physical access to the unlocked drives.	2023-12-15	4.6	Medium
CVE-2023-49584	sap - multiple products	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 793, allows an attacker to use HTTP verb POST on read-only service causing low impact on Confidentiality of the application.	2023-12-12	4.3	Medium
CVE-2023-20275	cisco - multiple products	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 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
CVE-2023-50765	jenkins - scriptler	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.	2023-12-13	4.3	Medium
CVE-2023-50769	jenkins - nexus_platform	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.	2023-12-13	4.3	Medium
CVE-2023-50772	jenkins - dingding_json_pusher	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
CVE-2023-50773	jenkins - dingding_json_pusher	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	4.3	Medium
CVE-2023-50775	jenkins - deployment_dashboard	A cross-site request forgery (CSRF) vulnerability in Jenkins Deployment Dashboard Plugin 1.0.10 and earlier allows attackers to copy jobs.	2023-12-13	4.3	Medium
CVE-2023-50776	jenkins - paaslane_estimate	Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier stores PaaSLane authentication tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with	2023-12-13	4.3	Medium

		Item/Extended Read permission or access to the Jenkins controller file system.			
CVE-2023-50777	jenkins - paaslane_estimate	Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier does not mask PaaSLane authentication tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2023-12-13	4.3	Medium
CVE-2023-50779	jenkins - paaslane_estimate	Missing permission checks in Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified URL using an attacker-specified token.	2023-12-13	4.3	Medium
CVE-2023-49877	ibm - virtualization_engine_ts7760_3957-vec_firmware	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-VED and 3957-VEC could allow a remote authenticated user to obtain sensitive information, caused by improper filtering of URLs. By submitting a specially crafted HTTP GET request, an attacker could exploit this vulnerability to view application source code, system configuration information, or other sensitive data related to the Management Interface. IBM X-Force ID: 272651.	2023-12-13	4.3	Medium
CVE-2023-49878	ibm - virtualization_engine_ts7760_3957-vec_firmware	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-VED and 3957-VEC could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 272652.	2023-12-13	4.3	Medium
CVE-2023-36878	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2023-12-15	4.3	Medium
CVE-2023-49578	sap - cloud_connector	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 impact on the availability and no impact on confidentiality or Integrity of the application.	2023-12-12	3.5	Low
CVE-2023-48608	adobe - multiple products	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 low-integrity impact within the application. Exploitation of this issue requires user interaction.	2023-12-15	3.5	Low
CVE-2023-48429	siemens - multiple products	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 admin to crash the server by sending a crafted request to the server. The server will automatically restart.	2023-12-12	2.7	Low
CVE-2023-48430	siemens - multiple products	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 malicious admin to crash the server by sending a crafted request to the API. The server will automatically restart.	2023-12-12	2.7	Low
CVE-2023-6793	paloaltonetworks - multiple products	An improper privilege management vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to revoke active XML API keys from the firewall and disrupt XML API usage.	2023-12-13	2.7	Low
CVE-2023-42874	apple - macos	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 keyboard.	2023-12-12	2.4	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.