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 ٩ يونيو إلى ١٥ يونيو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 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 9th of June to 15th of June. 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-2024-30299	Adobe	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	2024-06-13	10	Critical
CVE-2024-30080	Microsoft	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	2024-06-11	9.8	Critical
CVE-2024-26029	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-06-13	9.8	Critical
CVE-2024-34102	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.	2024-06-13	9.8	Critical
CVE-2024-30300	Adobe	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Information Exposure vulnerability (CWE-200) that could lead to privilege escalation. An attacker could exploit this vulnerability to gain access to sensitive information which may include system or user privileges. Exploitation of this issue does not require user interaction.	2024-06-13	9.8	Critical
CVE-2024-5671	Trellix	Insecure Deserialization in some workflows of the IPS Manager allows unauthenticated remote attackers to perform arbitrary code execution and access to the vulnerable Trellix IPS Manager.	2024-06-14	9.8	Critical
CVE-2024-36266	Siemens	A vulnerability has been identified in PowerSys (All versions < V3.11). The affected application insufficiently protects responses to authentication requests. This could allow a local attacker to bypass authentication, thereby gaining administrative privileges for the managed remote devices.	2024-06-11	9.3	Critical
CVE-2024-34108	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 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 does not require user interaction, but admin privileges are required	2024-06-13	9.1	Critical
CVE-2024-29855	Veeam	Hard-coded JWT secret allows authentication bypass in Veeam Recovery Orchestrator	2024-06-11	9	Critical
CVE-2024-30064	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	8.8	High
CVE-2024-30068	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	8.8	High
CVE-2024-30078	Microsoft	Windows Wi-Fi Driver Remote Code Execution Vulnerability	2024-06-11	8.8	High
CVE-2024-30097	Microsoft	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	2024-06-11	8.8	High
CVE-2024-30103	Microsoft	Microsoft Outlook Remote Code Execution Vulnerability	2024-06-11	8.8	High
CVE-2024-35249	Microsoft	Microsoft Dynamics 365 Business Central Remote Code Execution Vulnerability	2024-06-11	8.8	High

CVE-2024-5830	Google	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5831	Google	Use after free in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5832	Google	Use after free in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5833	Google	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5834	Google	Inappropriate implementation in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5835	Google	Heap buffer overflow in Tab Groups in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5836	Google	Inappropriate Implementation in DevTools in Google Chrome prior to 126.0.6478.54 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5837	Google	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5838	Google	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-06-11	8.8	High
CVE-2024-5841	Google	Use after free in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-5842	Google	Use after free in Browser UI in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-5844	Google	Heap buffer overflow in Tab Strip in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-5845	Google	Use after free in Audio in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-5846	Google	Use after free in PDFium in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-5847	Google	Use after free in PDFium in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	2024-06-11	8.8	High
CVE-2024-25949	Dell	Dell OS10 Networking Switches, versions10.5.6.x, 10.5.5.x, 10.5.4.x and 10.5.3.x ,contain an improper authorization vulnerability. A remote authenticated attacker could potentially exploit this vulnerability leading to escalation of privileges.	2024-06-12	8.8	High
CVE-2024-23299	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to break out of its sandbox.	2024-06-10	8.6	High
CVE-2024-35292	Siemens	A vulnerability has been identified in SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) (All versions), SIMATIC S7-200 SMART	2024-06-11	8.2	High

		CPU ST60 (6ES7288-1ST60-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) (All versions). Affected devices are using a predictable IP ID sequence number. This leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.			
CVE-2024-34104	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access, leading to both confidentiality and integrity impact. Exploitation of this issue does not require user interaction.	2024-06-13	8.2	High
CVE-2024-37325	Microsoft	Azure Science Virtual Machine (DSVM) Elevation of Privilege Vulnerability	2024-06-11	8.1	High
CVE-2024-34103	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction, but attack complexity is high.	2024-06-13	8.1	High
CVE-2024-30074	Microsoft	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	2024-06-11	8	High
CVE-2024-30075	Microsoft	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	2024-06-11	8	High
CVE-2024-30077	Microsoft	Windows OLE Remote Code Execution Vulnerability	2024-06-11	8	High
CVE-2024-36502	Huawei	Out-of-bounds read vulnerability in the audio module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	7.9	High
CVE-2024-36971	Linux	In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advice() uses the wrong order. Given that ip6_negative_advice() has special logic against RTF_CACHE, this means each of the three - >negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advice(), there is no need to duplicate it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets.	2024-06-10	7.8	High
CVE-2022-32897	Apple	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted tiff file may lead to arbitrary code execution.	2024-06-10	7.8	High
CVE-2022-48683	Apple	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13. An app may be able to break out of its sandbox.	2024-06-10	7.8	High
CVE-2024-35206	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application does not expire the session. This could allow an attacker to get unauthorized access.	2024-06-11	7.8	High
CVE-2024-35207	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The web interface of the affected devices are vulnerable to Cross-Site Request Forgery(CSRF) attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.	2024-06-11	7.8	High
CVE-2024-35303	Siemens	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0012), Tecnomatix Plant Simulation V2404 (All versions < V2404.0001). The affected applications contain a type confusion vulnerability while parsing specially crafted MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22958)	2024-06-11	7.8	High
CVE-2024-23110	Fortinet	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0	2024-06-11	7.8	High

		through 6.4.14, 6.2.0 through 6.2.15, 6.0 all versions allows attacker to execute unauthorized code or commands via specially crafted commands			
CVE-2024-30062	Microsoft	Windows Standards-Based Storage Management Service Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-30072	Microsoft	Microsoft Event Trace Log File Parsing Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-30082	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30085	Microsoft	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30086	Microsoft	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30087	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30089	Microsoft	Microsoft Streaming Service Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30091	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-30094	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-30095	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-30100	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-30104	Microsoft	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.8	High
CVE-2024-35250	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-06-11	7.8	High
CVE-2024-28964	Dell	Dell Common Event Enabler, version 8.9.10.0 and prior, contain an insecure deserialization vulnerability in CAVATools. A local unauthenticated attacker could potentially exploit this vulnerability, leading to arbitrary code execution in the context of the logged in user. Exploitation of this issue requires a victim to open a malicious file.	2024-06-12	7.8	High
CVE-2024-20753	Adobe	Photoshop Desktop versions 24.7.3, 25.7 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.	2024-06-13	7.8	High
CVE-2024-34115	Adobe	Substance3D - Stager versions 2.1.4 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.	2024-06-13	7.8	High
CVE-2024-32896	Google	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-06-13	7.8	High
CVE-2024-36500	Huawei	Privilege escalation vulnerability in the AMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-06-14	7.8	High
CVE-2024-35209	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is allowing HTTP methods like PUT and Delete. This could allow an attacker to modify unauthorized files.	2024-06-11	7.5	High
CVE-2024-35212	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application lacks input validation due to which an attacker can gain access to the Database entries.	2024-06-11	7.5	High
CVE-2024-26010	Fortinet	A stack-based buffer overflow in Fortinet FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiWeb, FortiAuthenticator, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.1 through 7.0.3, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-06-11	7.5	High
CVE-2024-30070	Microsoft	DHCP Server Service Denial of Service Vulnerability	2024-06-11	7.5	High
CVE-2024-30083	Microsoft	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-06-11	7.5	High
CVE-2024-30101	Microsoft	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.5	High
CVE-2024-35252	Microsoft	Azure Storage Movement Client Library Denial of Service Vulnerability	2024-06-11	7.5	High
CVE-2024-30472	Dell	Telemetry Dashboard v1.0.0.8 for Dell ThinOS 2402 contains a sensitive information disclosure vulnerability. An unauthenticated user with local access to the device could exploit this vulnerability leading to information disclosure.	2024-06-13	7.5	High
CVE-2024-34112	Adobe	ColdFusion versions 2023u7, 2021u13 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could exploit this	2024-06-13	7.5	High

		vulnerability to gain unauthorized access to sensitive files or data. Exploitation of this issue does not require user interaction.			
CVE-2024-32858	Dell	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	High
CVE-2024-32859	Dell	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	High
CVE-2024-32860	Dell	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	High
CVE-2024-37131	Dell	SCG Policy Manager, all versions, contains an overly permissive Cross-Origin Resource Policy (CORP) vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious actions on the application in the context of the authenticated user.	2024-06-13	7.5	High
CVE-2024-4696	Lenovo	A privilege escalation vulnerability was reported in Lenovo Service Bridge prior to version 5.0.2.17 that could allow operating system commands to be executed if a specially crafted link is visited.	2024-06-13	7.5	High
CVE-2024-27275	IBM	IBM i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability caused by an insufficient authority requirement. A local user without administrator privilege can configure a physical file trigger to execute with the privileges of a user socially engineered to access the target file. The correction is to require administrator privilege to configure trigger support. IBM X-Force ID: 285203.	2024-06-15	7.4	High
CVE-2024-37130	Dell	Dell OpenManage Server Administrator, versions 11.0.1.0 and prior, contains a Local Privilege Escalation vulnerability via XSL Hijacking. A local low-privileged malicious user could potentially exploit this vulnerability and escalate their privilege to the admin user and gain full control of the machine. Exploitation may lead to a complete system compromise.	2024-06-11	7.3	High
CVE-2024-30093	Microsoft	Windows Storage Elevation of Privilege Vulnerability	2024-06-11	7.3	High
CVE-2024-30102	Microsoft	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.3	High
CVE-2024-35248	Microsoft	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	2024-06-11	7.3	High
CVE-2024-36503	Huawei	Memory management vulnerability in the Gralloc module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	7.3	High
CVE-2024-34109	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 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 does not require user interaction, but admin privileges are required.	2024-06-13	7.2	High
CVE-2024-34110	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. A high-privilege attacker could exploit this vulnerability by uploading a malicious file to the system, which could then be executed. Exploitation of this issue does not require user interaction.	2024-06-13	7.2	High
CVE-2022-48578	Apple	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5. Processing an AppleScript may result in unexpected termination or disclosure of process memory.	2024-06-10	7.1	High
CVE-2024-35254	Microsoft	Azure Monitor Agent Elevation of Privilege Vulnerability	2024-06-11	7.1	High
CVE-2024-30084	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-06-11	7	High
CVE-2024-30088	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	7	High
CVE-2024-30090	Microsoft	Microsoft Streaming Service Elevation of Privilege Vulnerability	2024-06-11	7	High
CVE-2024-30099	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	7	High
CVE-2024-35265	Microsoft	Windows Perception Service Elevation of Privilege Vulnerability	2024-06-11	7	High
CVE-2024-23111	Fortinet	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.	2024-06-11	6.8	Medium
CVE-2024-30076	Microsoft	Windows Container Manager Service Elevation of Privilege Vulnerability	2024-06-11	6.8	Medium
CVE-2024-0160	Dell	Dell Client Platform contains an incorrect authorization vulnerability. An attacker with physical access to the system could potentially exploit this vulnerability by bypassing BIOS authorization to modify settings in the BIOS.	2024-06-12	6.8	Medium
CVE-2024-36499	Huawei	Vulnerability of unauthorized screenshot capturing in the WMS module	2024-06-14	6.8	Medium

		Impact: Successful exploitation of this vulnerability may affect service confidentiality.			
CVE-2024-5731	Trellix	A vulnerability in the IPS Manager, Central Manager, and Local Manager communication workflow allows an attacker to control the destination of a request by manipulating the parameter, thereby leveraging sensitive information.	2024-06-14	6.8	Medium
CVE-2023-46720	Fortinet	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	2024-06-11	6.7	Medium
CVE-2024-29060	Microsoft	Visual Studio Elevation of Privilege Vulnerability	2024-06-11	6.7	Medium
CVE-2024-30063	Microsoft	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	2024-06-11	6.7	Medium
CVE-2023-45188	IBM	IBM Engineering Lifecycle Optimization Publishing 7.0.2 and 7.03 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially crafted request, a remote attacker could exploit this vulnerability to upload a malicious file, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 268751.	2024-06-09	6.5	Medium
CVE-2024-35210	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is not enforcing HSTS. This could allow an attacker to perform downgrade attacks exposing confidential information.	2024-06-11	6.5	Medium
CVE-2024-35211	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server, after a successful login, sets the session cookie on the browser, without applying any security attributes (such as “Secure”, “HttpOnly”, or “SameSite”).	2024-06-11	6.5	Medium
CVE-2023-23775	Fortinet	Multiple improper neutralization of special elements used in SQL commands ('SQL Injection') vulnerabilities [CWE-89] in FortiSOAR 7.2.0 and before 7.0.3 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted strings parameters.	2024-06-11	6.5	Medium
CVE-2024-5839	Google	Inappropriate Implementation in Memory Allocator in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-06-11	6.5	Medium
CVE-2024-5840	Google	Policy bypass in CORS in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2024-06-11	6.5	Medium
CVE-2024-5843	Google	Inappropriate implementation in Downloads in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to obfuscate security UI via a malicious file. (Chromium security severity: Medium)	2024-06-11	6.5	Medium
CVE-2024-31881	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash when using a specially crafted query on certain columnar tables by an authenticated user. IBM X-Force ID: 287613.	2024-06-12	6.5	Medium
CVE-2024-34111	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted request to the server, which could then cause the server to execute arbitrary code. Exploitation of this issue does not require user interaction.	2024-06-13	6.5	Medium
CVE-2024-35208	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server stored the password in cleartext. This could allow attacker in a privileged position to obtain access passwords.	2024-06-11	6.3	Medium
CVE-2024-34129	Adobe	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to access files and directories that are outside the restricted directory and also to overwrite arbitrary files. Exploitation of this issue does not requires user interaction and attack complexity is high.	2024-06-13	6.3	Medium
CVE-2024-34113	Adobe	ColdFusion versions 2023u7, 2021u13 and earlier are affected by a Weak Cryptography for Passwords vulnerability that could result in a security feature bypass. This vulnerability arises due to the use of insufficiently strong cryptographic algorithms or flawed implementation that compromises the confidentiality of password data. An attacker could exploit this weakness to decrypt or guess passwords, potentially gaining unauthorized access to protected resources. Exploitation of this issue does not require user interaction.	2024-06-13	6.2	Medium

CVE-2024-36216	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	6.1	Medium
CVE-2024-33500	Siemens	A vulnerability has been identified in Mendix Applications using Mendix 10 (All versions < V10.11.0), Mendix Applications using Mendix 10 (V10.6) (All versions < V10.6.9), Mendix Applications using Mendix 9 (All versions >= V9.3.0 < V9.24.22). Affected applications could allow users with the capability to manage a role to elevate the access rights of users with that role. Successful exploitation requires to guess the id of a target role which contains the elevated access rights.	2024-06-11	5.9	Medium
CVE-2024-5465	Huawei	Function vulnerabilities in the Calendar module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	5.9	Medium
CVE-2024-35263	Microsoft	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2024-06-11	5.7	Medium
CVE-2024-36501	Huawei	Memory management vulnerability in the boottime module Impact: Successful exploitation of this vulnerability can affect integrity.	2024-06-14	5.6	Medium
CVE-2023-40389	Apple	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data.	2024-06-10	5.5	Medium
CVE-2024-27792	Apple	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4. An app may be able to access user-sensitive data.	2024-06-10	5.5	Medium
CVE-2024-30065	Microsoft	Windows Themes Denial of Service Vulnerability	2024-06-11	5.5	Medium
CVE-2024-30066	Microsoft	Winlogon Elevation of Privilege Vulnerability	2024-06-11	5.5	Medium
CVE-2024-30067	Microsoft	Winlogon Elevation of Privilege Vulnerability	2024-06-11	5.5	Medium
CVE-2024-30096	Microsoft	Windows Cryptographic Services Information Disclosure Vulnerability	2024-06-11	5.5	Medium
CVE-2024-35255	Microsoft	Azure Identity Libraries and Microsoft Authentication Library Elevation of Privilege Vulnerability	2024-06-11	5.5	Medium
CVE-2024-30276	Adobe	Audition versions 24.2, 23.6.4 and earlier Answer: 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.	2024-06-13	5.5	Medium
CVE-2024-30285	Adobe	Audition versions 24.2, 23.6.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service condition. An attacker could exploit this vulnerability to crash the application, leading to a denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-06-13	5.5	Medium
CVE-2024-30278	Adobe	Media Encoder versions 23.6.5, 24.3 and earlier Answer: 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.	2024-06-13	5.5	Medium
CVE-2024-34116	Adobe	Creative Cloud Desktop versions 6.1.0.587 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to load and execute malicious libraries, leading to arbitrary file delete. Exploitation of this issue requires user interaction.	2024-06-13	5.5	Medium
CVE-2024-34130	Adobe	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could exploit this vulnerability to access confidential information. Exploitation of this issue does not require user interaction.	2024-06-13	5.5	Medium
CVE-2024-20769	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-20784	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26036	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	2024-06-13	5.4	Medium

		victim’s browser when they browse to the page containing the vulnerable field.			
CVE-2024-26037	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	Medium
CVE-2024-26039	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-26053	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-26054	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26055	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	Medium
CVE-2024-26057	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	Medium
CVE-2024-26058	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	Medium
CVE-2024-26060	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26066	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26068	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26070	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26071	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-26072	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	Medium
CVE-2024-26074	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26075	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26077	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26078	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26081	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26082	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26083	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26085	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26086	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26088	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26089	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	2024-06-13	5.4	Medium
CVE-2024-26090	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	Medium

CVE-2024-26091	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	Medium
CVE-2024-26092	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26093	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26095	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26110	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26111	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26113	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26114	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26115	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26116	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26117	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-26121	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-26123	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-34119	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-34120	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36141	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are 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.	2024-06-13	5.4	Medium
CVE-2024-36142	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36143	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36144	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36146	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36147	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36148	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36149	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36150	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36151	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	2024-06-13	5.4	Medium
CVE-2024-36152	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36153	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-36154	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36155	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36156	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36157	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36158	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36159	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36160	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36161	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36162	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36163	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36164	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36165	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36166	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-36167	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36168	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36169	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36170	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36171	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36172	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36173	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36174	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36175	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36176	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36177	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36178	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36179	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-36180	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36181	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application.	2024-06-13	5.4	Medium
CVE-2024-36182	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36183	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	Medium
CVE-2024-36184	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a specially crafted form.	2024-06-13	5.4	Medium
CVE-2024-36185	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36186	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36187	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36188	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36189	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36190	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-36191	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36192	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	2024-06-13	5.4	Medium

		could be abused by an 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.			
CVE-2024-36193	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36194	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36195	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36196	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36197	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-36198	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36199	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36200	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36201	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36202	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36203	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36204	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36205	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	2024-06-13	5.4	Medium

		could be abused by an 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.			
CVE-2024-36206	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-36207	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36208	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36209	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36210	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	2024-06-13	5.4	Medium
CVE-2024-36211	Adobe	Adobe Experience Manager versions 6.5.20 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.	2024-06-13	5.4	Medium
CVE-2024-36212	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36213	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36214	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36215	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36217	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36218	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36219	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium

CVE-2024-36220	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	Medium
CVE-2024-36221	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36222	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-36224	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	Medium
CVE-2024-36225	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36227	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	Medium
CVE-2024-36228	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-36229	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	Medium
CVE-2024-36230	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	Medium
CVE-2024-36231	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	Medium
CVE-2024-36232	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	Medium
CVE-2024-36233	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute	2024-06-13	5.4	Medium

		arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link.			
CVE-2024-36234	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	Medium
CVE-2024-36235	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	Medium
CVE-2024-36236	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	Medium
CVE-2024-36238	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to interact with a maliciously crafted web page.	2024-06-13	5.4	Medium
CVE-2024-36239	Adobe	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	Medium
CVE-2024-28965	Dell	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal enable REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain Internal APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	Medium
CVE-2024-28966	Dell	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	Medium
CVE-2024-28967	Dell	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal maintenance REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	Medium
CVE-2024-28968	Dell	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for internal email and collection settings REST APIs (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	Medium
CVE-2024-29168	Dell	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal assets REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing potential unauthorized access and modification of application data.	2024-06-13	5.4	Medium
CVE-2024-29169	Dell	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal audit REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the	2024-06-13	5.4	Medium

		application's backend database causing potential unauthorized access and modification of application data.			
CVE-2024-30057	Microsoft	Microsoft Edge for iOS Spoofing Vulnerability	2024-06-13	5.4	Medium
CVE-2024-30058	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-13	5.4	Medium
CVE-2022-32933	Apple	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.5. A website may be able to track the websites a user visited in Safari private browsing mode.	2024-06-10	5.3	Medium
CVE-2024-28762	IBM	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 285246.	2024-06-12	5.3	Medium
CVE-2023-29267	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287612.	2024-06-12	5.3	Medium
CVE-2024-34106	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to gain unauthorized access or perform actions with the privileges of another user. Exploitation of this issue does not require user interaction.	2024-06-13	5.3	Medium
CVE-2024-34107	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-06-13	5.3	Medium
CVE-2024-21988	NetApp	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.7.0.9 and 11.8.0.5 are susceptible to disclosure of sensitive information via complex MiTM attacks due to a vulnerability in the SSH cryptographic implementation.	2024-06-14	5.3	Medium
CVE-2024-32856	Dell	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-06-13	5.1	Medium
CVE-2023-50763	Siemens	A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of affected products, if configured to allow the import of PKCS12 containers, could end up in an infinite loop when processing incomplete certificate chains. This could allow an authenticated remote attacker to create a denial of service condition by importing specially crafted PKCS12 containers.	2024-06-11	4.9	Medium
CVE-2024-26049	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a 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.	2024-06-13	4.8	Medium
CVE-2024-34105	Adobe	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin 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.	2024-06-13	4.8	Medium
CVE-2024-30052	Microsoft	Visual Studio Remote Code Execution Vulnerability	2024-06-11	4.7	Medium
CVE-2024-30069	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-06-11	4.7	Medium
CVE-2024-28970	Dell	Dell Client BIOS contains an Out-of-bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to platform denial of service.	2024-06-12	4.7	Medium
CVE-2024-35253	Microsoft	Microsoft Azure File Sync Elevation of Privilege Vulnerability	2024-06-11	4.4	Medium

CVE-2024-25052	IBM	IBM Jazz Reporting Service 7.0.3 stores user credentials in plain clear text which can be read by an admin user. IBM X-Force ID: 283363.	2024-06-13	4.4	Medium
CVE-2024-31495	Fortinet	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiPortal versions 7.0.0 through 7.0.6 and version 7.2.0 allows privileged user to obtain unauthorized information via the report download functionality.	2024-06-11	4.3	Medium
CVE-2024-28969	Dell	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources.	2024-06-13	4.3	Medium
CVE-2024-38083	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-13	4.3	Medium
CVE-2024-4176	Trellix	An Cross site scripting vulnerability in the EDR XConsole before this release allowed an attacker to potentially leverage an XSS/HTML-Injection using command line variables. A malicious threat actor could execute commands on the victim's browser for sending carefully crafted malicious links to the EDR XConsole end user.	2024-06-13	4.1	Medium
CVE-2024-22333	IBM	IBM Maximo Asset Management 7.6.1.3 and IBM Maximo Application Suite 8.10 and 8.11 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 279973.	2024-06-13	4	Medium
CVE-2024-5464	Huawei	Vulnerability of insufficient permission verification in the NearLink module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-06-14	4	Medium
CVE-2024-26126	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	Low
CVE-2024-26127	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	Low
CVE-2024-36226	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	Low
CVE-2023-38533	Siemens	A vulnerability has been identified in TIA Administrator (All versions < V3 SP2). The affected component creates temporary download files in a directory with insecure permissions. This could allow any authenticated attacker on Windows to disrupt the update process.	2024-06-11	3.3	Low
CVE-2024-31870	IBM	IBM Db2 for i 7.2, 7.3, 7.4, and 7.5 supplies user defined table function is vulnerable to user enumeration by a local authenticated attacker, without having authority to the related *USRPRF objects. This can be used by a malicious actor to gather information about users that can be targeted in further attacks. IBM X-Force ID: 287174.	2024-06-15	3.3	Low
CVE-2024-21754	Fortinet	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.	2024-06-11	1.8	Low

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.

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.