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 ١٠ سبتمبر إلى ١٧ سبتمبر. 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 10th of September to 17th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-40622	sap - multiple products	SAP BusinessObjects Business Intelligence Platform (Promotion Management) - versions 420, 430, under certain condition allows an authenticated attacker to view sensitive information which is otherwise restricted. On successful exploitation, the attacker can completely compromise the application causing high impact on confidentiality, integrity, and availability.	2023-09-12	9.9	Critical
CVE-2023-35681	google - android	In eatt_l2cap_reconfig_completed of eatt_impl.h, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	9.8	Critical
CVE-2023-40309	sap - multiple products	SAP CommonCryptoLib does not perform necessary authentication checks, which may result in missing or wrong authorization checks for an authenticated user, resulting in escalation of privileges. Depending on the application and the level of privileges acquired, an attacker could abuse functionality restricted to a particular user group as well as read, modify or delete restricted data.	2023-09-12	9.8	Critical
CVE-2023-29332	microsoft - azure_kubernetes_ service	Microsoft Azure Kubernetes Service Elevation of Privilege Vulnerability	2023-09-12	9.8	Critical
CVE-2023-36758	microsoft - visual_studio_2022	Visual Studio Elevation of Privilege Vulnerability	2023-09-12	9.8	Critical
CVE-2023-36765	microsoft - office	Microsoft Office Elevation of Privilege Vulnerability	2023-09-12	9.8	Critical
CVE-2023-4501	microfocus - multiple products	User authentication with username and password credentials is ineffective in OpenText (Micro Focus) Visual COBOL, COBOL Server, Enterprise Developer, and Enterprise Server (including product variants such as Enterprise Test Server), versions 7.0 patch updates 19 and 20, 8.0 patch updates 8 and 9, and 9.0 patch update 1, when LDAP-based authentication is used with certain configurations. When the vulnerability is active, authentication succeeds with any valid username, regardless of whether the password is correct; it may also succeed with an invalid username (and any password). This allows an attacker with access to the product to impersonate any user. Mitigations: The issue is corrected in the upcoming patch update for each affected product. Product overlays and workaround instructions are available through OpenText Support. The vulnerable configurations are believed to be uncommon. Administrators can test for the vulnerability in their installations by attempting to sign on to a Visual COBOL or Enterprise Server component such as ESCWA using a valid username and incorrect password.	2023-09-12	9.8	Critical
CVE-2023-38204	adobe - multiple products	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code	2023-09-14	9.8	Critical

		execution. Exploitation of this issue does not require user interaction.			
CVE-2023-30909	hp - oneview	A remote authentication bypass issue exists in some OneView APIs.	2023-09-14	9.8	Critical
CVE-2023-0923	redhat - openshift_data_science	A flaw was found in the Kubernetes service for notebooks in RHODS, where it does not prevent pods from other namespaces and applications from making requests to the Jupyter API. This flaw can lead to file content exposure and other issues.	2023-09-15	9.8	Critical
CVE-2023-36735	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-09-15	9.6	Critical
CVE-2023-4582	mozilla - multiple products	Due to large allocation checks in Angle for glsl shaders being too lenient a buffer overflow could have occured when allocating too much private shader memory on mac OS. *This bug only affects Firefox on macOS. Other operating systems are unaffected.* This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.	2023-09-11	8.8	High
CVE-2023-4584	mozilla - multiple products	Memory safety bugs present in Firefox 116, Firefox ESR 102.14, Firefox ESR 115.1, Thunderbird 102.14, and Thunderbird 115.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	8.8	High
CVE-2023-4585	mozilla - multiple products	Memory safety bugs present in Firefox 116, Firefox ESR 115.1, and Thunderbird 115.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.	2023-09-11	8.8	High
CVE-2022-1415	redhat - multiple products	A flaw was found where some utility classes in Drools core did not use proper safeguards when deserializing data. This flaw allows an authenticated attacker to construct malicious serialized objects (usually called gadgets) and achieve code execution on the server.	2023-09-11	8.8	High
CVE-2023-35658	google - multiple products	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible privilege escalation due to a use after free. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	8.8	High
CVE-2023-35673	google - multiple products	In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	8.8	High
CVE-2023-35684	google - multiple products	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to an integer overflow. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	8.8	High
CVE-2023-40726	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The affected application server responds with sensitive information about the server. This could allow an attacker to directly access the database.	2023-09-12	8.8	High
CVE-2023-40730	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The QMS.Mobile module of the affected application lacks sufficient authorization checks. This could allow an attacker to access confidential information, perform administrative functions, or lead to a denial-of-service condition.	2023-09-12	8.8	High
CVE-2023-40731	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The affected application allows users to upload arbitrary file types. This could allow an attacker to upload malicious files, that could potentially lead to code tampering.	2023-09-12	8.8	High
CVE-2023-4863	google - chrome	Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	2023-09-12	8.8	High
CVE-2023-33136	microsoft - multiple products	Azure DevOps Server Remote Code Execution Vulnerability	2023-09-12	8.8	High
CVE-2023-36764	microsoft - multiple products	Microsoft SharePoint Server Elevation of Privilege Vulnerability	2023-09-12	8.8	High
CVE-2023-38146	microsoft - multiple products	Windows Themes Remote Code Execution Vulnerability	2023-09-12	8.8	High
CVE-2023-38147	microsoft - multiple products	Windows Miracast Wireless Display Remote Code Execution Vulnerability	2023-09-12	8.8	High

CVE-2023-38148	microsoft - multiple products	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability	2023-09-12	8.8	High
CVE-2023-4918	redhat - keycloak	A flaw was found in the Keycloak package, more specifically org.keycloak.userprofile. When a user registers itself through registration flow, the "password" and "password-confirm" field from the form will occur as regular user attributes. All users and clients with proper rights and roles are able to read users attributes, allowing a malicious user with minimal access to retrieve the users passwords in clear text, jeopardizing their environment.	2023-09-12	8.8	High
CVE-2022-35849	fortinet - multiple products	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiADC 7.1.0 through 7.1.1, 7.0.0 through 7.0.3, 6.2.0 through 6.2.5 and 6.1.0 all versions may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	2023-09-13	8.8	High
CVE-2023-34984	fortinet - multiple products	A protection mechanism failure in Fortinet FortiWeb 7.2.0 through 7.2.1, 7.0.0 through 7.0.6, 6.4.0 through 6.4.3, 6.3.6 through 6.3.23 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2023-09-13	8.8	High
CVE-2023-36634	fortinet - multiple products	An incomplete filtering of one or more instances of special elements vulnerability [CWE-792] in the command line interpreter of FortiAP-U 7.0.0, 6.2.0 through 6.2.5, 6.0 all versions, 5.4 all versions may allow an authenticated attacker to list and delete arbitrary files and directory via specially crafted command arguments.	2023-09-13	8.8	High
CVE-2023-4576	mozilla - multiple products	On Windows, an integer overflow could occur in `RecordedSourceSurfaceCreation` which resulted in a heap buffer overflow potentially leaking sensitive data that could have led to a sandbox escape. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	8.6	High
CVE-2023-38155	microsoft - multiple products	Azure DevOps Server Remote Code Execution Vulnerability	2023-09-12	8.1	High
CVE-2023-36744	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-09-12	8	High
CVE-2023-36745	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-09-12	8	High
CVE-2023-36756	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-09-12	8	High
CVE-2023-36757	microsoft - multiple products	Microsoft Exchange Server Spoofing Vulnerability	2023-09-12	8	High
CVE-2019-16470	adobe - multiple products	Adobe Acrobat Reader versions 2019.021.20056 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2019-16471	adobe - multiple products	Adobe Acrobat Reader versions 2019.021.20056 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-28831	adobe - multiple products	Adobe InDesign versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-28832	adobe - multiple products	Adobe InDesign versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-28833	adobe - multiple products	Adobe InDesign versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-28834	adobe - multiple products	Adobe InCopy versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-28835	adobe - multiple products	Adobe InCopy versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user.	2023-09-11	7.8	High

		Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2022-28836	adobe - multiple products	Adobe InCopy versions 17.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-34224	adobe - multiple products	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2022-34227	adobe - multiple products	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	7.8	High
CVE-2023-35665	google - multiple products	In multiple files, there is a possible way to import a contact from another user due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35666	google - multiple products	In bta_av_rc_msg of bta_av_act.cc, there is a possible use after free 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 not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35667	google - multiple products	In updateList of NotificationAccessSettings.java, there is a possible way to hide approved notification listeners in the settings 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 not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35669	google - multiple products	In checkKeyIntentParceledCorrectly of AccountManagerService.java, there is a possible way to control other running activities due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35670	google - multiple products	In computeValuesFromData of FileUtils.java, there is a possible way to insert files to other apps' external private directories due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35674	google - multiple products	In onCreate of WindowState.java, there is a possible way to launch a background activity 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 not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35676	google - multiple products	In createQuickShareAction of SaveImageInBackgroundTask.java, there is a possible way to trigger a background activity launch due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35682	google - multiple products	In hasPermissionForActivity of PackageManagerHelper.java, there is a possible way to start arbitrary components due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2023-09-11	7.8	High
CVE-2023-35687	google - multiple products	In MtpPropertyValue of MtpProperty.h, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	7.8	High
CVE-2023-41990	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in tvOS 16.3, iOS 16.3 and iPadOS 16.3, macOS Monterey 12.6.8, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Ventura 13.2, watchOS 9.3. Processing a font file may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.1.	2023-09-12	7.8	High
CVE-2023-3039	dell - sd_rom_utility	SD ROM Utility, versions prior to 1.0.2.0 contain an Improper Access Control vulnerability. A low-privileged malicious user may potentially exploit this vulnerability to perform arbitrary code execution with limited access.	2023-09-12	7.8	High
CVE-2023-38070	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application is vulnerable to stack-based buffer overflow	2023-09-12	7.8	High

		while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20818)			
CVE-2023-38071	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20824)	2023-09-12	7.8	High
CVE-2023-38072	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20825)	2023-09-12	7.8	High
CVE-2023-38073	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20826)	2023-09-12	7.8	High
CVE-2023-38074	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20840)	2023-09-12	7.8	High
CVE-2023-38075	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted WRL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20842)	2023-09-12	7.8	High
CVE-2023-38076	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.1), Teamcenter Visualization V13.3 (All versions < V13.3.0.12), Teamcenter Visualization V14.0 (All versions), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.1). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21041)	2023-09-12	7.8	High
CVE-2023-40727	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The QMS.Mobile module of the affected application uses weak outdated application signing mechanism. This could allow an attacker to tamper the application code.	2023-09-12	7.8	High
CVE-2023-40728	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The QMS.Mobile module of the affected application stores sensitive application data in an external insecure storage. This could allow an attacker to alter content, leading to arbitrary code execution or denial-of-service condition.	2023-09-12	7.8	High
CVE-2023-41032	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.253), Parasolid V35.1 (All versions < V35.1.184), Parasolid V36.0 (All versions < V36.0.142). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21263)	2023-09-12	7.8	High
CVE-2023-41033	siemens - multiple products	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.260), Parasolid V35.1 (All versions < V35.1.246), Parasolid	2023-09-12	7.8	High

متاح

		V36.0 (All versions < V36.0.156). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21266)			
CVE-2023-41846	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to memory corruption while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	2023-09-12	7.8	High
CVE-2023-35355	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-36739	microsoft - 3d_viewer	3D Viewer Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36740	microsoft - 3d_viewer	3D Viewer Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36742	microsoft - visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36760	microsoft - 3d_viewer	3D Viewer Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36770	microsoft - 3d_builder	3D Builder Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36771	microsoft - 3d_builder	3D Builder Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36772	microsoft - 3d_builder	3D Builder Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36773	microsoft - 3d_builder	3D Builder Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36788	microsoft - .net_framework	.NET Framework Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36792	microsoft - .net_framework	Visual Studio Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36793	microsoft - .net_framework	Visual Studio Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36794	microsoft - .net_framework	Visual Studio Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36796	microsoft - .net_framework	Visual Studio Remote Code Execution Vulnerability	2023-09-12	7.8	High
CVE-2023-36802	microsoft - multiple products	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-36804	microsoft - multiple products	Windows GDI Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38139	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38141	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38142	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38143	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38144	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38150	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38161	microsoft - multiple products	Windows GDI Elevation of Privilege Vulnerability	2023-09-12	7.8	High
CVE-2023-38163	microsoft - windows_defender_security_intelligence_updates	Windows Defender Attack Surface Reduction Security Feature Bypass	2023-09-12	7.8	High
CVE-2023-4921	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d8.	2023-09-12	7.8	High
CVE-2023-26369	adobe - multiple products	Acrobat Reader versions 23.003.20284 (and earlier), 20.005.30516 (and earlier) and 20.005.30514 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-13	7.8	High

CVE-2023-36642	fortinet - fortitester	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 3.0.0 through 7.2.3 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	2023-09-13	7.8	High
CVE-2023-40717	fortinet - fortitester	A use of hard-coded credentials vulnerability [CWE-798] in FortiTester 2.3.0 through 7.2.3 may allow an attacker who managed to get a shell on the device to access the database via shell commands.	2023-09-13	7.8	High
CVE-2023-20236	cisco - ios_xr	A vulnerability in the iPXE boot function of Cisco IOS XR software could allow an authenticated, local attacker to install an unverified software image on an affected device. This vulnerability is due to insufficient image verification. An attacker could exploit this vulnerability by manipulating the boot parameters for image verification during the iPXE boot process on an affected device. A successful exploit could allow the attacker to boot an unverified software image on the affected device.	2023-09-13	7.8	High
CVE-2023-41267	apache - airflow_hdfs_provider	In the Apache Airflow HDFS Provider, versions prior to 4.1.1, a documentation info pointed users to an install incorrect pip package. As this package name was unclaimed, in theory, an attacker could claim this package and provide code that would be executed when this package was installed. The Airflow team has since taken ownership of the package (neutralizing the risk), and fixed the doc strings in version 4.1.1	2023-09-14	7.8	High
CVE-2023-4516	schneider-electric - interactive_graphical_scada_system	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the IGSS Update Service that could allow a local attacker to change update source, potentially leading to remote code execution when the attacker force an update containing malicious content.	2023-09-14	7.8	High
CVE-2023-38557	siemens - spectrum_power_7	A vulnerability has been identified in Spectrum Power 7 (All versions < V23Q3). The affected product assigns improper access rights to the update script. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	2023-09-14	7.8	High
CVE-2023-4583	mozilla - multiple products	When checking if the Browsing Context had been discarded in `HttpBaseChannel`, if the load group was not available then it was assumed to have already been discarded which was not always the case for private channels after the private session had ended. This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.	2023-09-11	7.5	High
CVE-2023-40440	apple - macos	This issue was addressed with improved state management of S/MIME encrypted emails. This issue is fixed in macOS Monterey 12.6.8. A S/MIME encrypted email may be inadvertently sent unencrypted.	2023-09-12	7.5	High
CVE-2023-40308	sap - multiple products	SAP CommonCryptoLib allows an unauthenticated attacker to craft a request, which when submitted to an open port causes a memory corruption error in a library which in turn causes the target component to crash making it unavailable. There is no ability to view or modify any information.	2023-09-12	7.5	High
CVE-2023-28831	siemens - simatic_cloud_connect_7_cc712_firmware	The ANSI C OPC UA SDK contains an integer overflow vulnerability that could cause the application to run into an infinite loop during certificate validation. This could allow an unauthenticated remote attacker to create a denial of service condition by sending a specially crafted certificate.	2023-09-12	7.5	High
CVE-2023-36763	microsoft - multiple products	Microsoft Outlook Information Disclosure Vulnerability	2023-09-12	7.5	High
CVE-2023-38149	microsoft - multiple products	Windows TCP/IP Denial of Service Vulnerability	2023-09-12	7.5	High
CVE-2023-38162	microsoft - multiple products	DHCP Server Service Denial of Service Vulnerability	2023-09-12	7.5	High
CVE-2023-39208	zoom - zoom	Improper input validation in Zoom Desktop Client for Linux before version 5.15.10 may allow an unauthenticated user to conduct a denial of service via network access.	2023-09-12	7.5	High
CVE-2023-41081	apache - tomcat_connectors	The mod_jk component of Apache Tomcat Connectors in some circumstances, such as when a configuration included "JkOptions +ForwardDirectories" but the configuration did not provide explicit mounts for all possible proxied requests, mod_jk would use an implicit mapping and map the request to the first defined worker. Such an implicit mapping could result in the unintended exposure of the status worker and/or bypass security constraints configured in httpd. As of JK 1.2.49, the implicit mapping functionality has been removed and all mappings must now be via	2023-09-13	7.5	High

متاح

		explicit configuration. Only mod_jk is affected by this issue. The ISAPI redirector is not affected. This issue affects Apache Tomcat Connectors (mod_jk only): from 1.2.0 through 1.2.48. Users are recommended to upgrade to version 1.2.49, which fixes the issue.			
CVE-2023-4801	proofpoint - insider_threat_management	An improper certification validation vulnerability in the Insider Threat Management (ITM) Agent for MacOS could be used by an anonymous actor on an adjacent network to establish a man-in-the-middle position between the agent and the ITM server after the agent has registered. All versions prior to 7.14.3.69 are affected. Agents for Windows, Linux, and Cloud are unaffected.	2023-09-13	7.5	High
CVE-2023-20191	cisco - multiple products	A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incomplete support for this feature. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device. There are workarounds that address this vulnerability. This advisory is part of the September 2023 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: September 2023 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication .	2023-09-13	7.5	High
CVE-2023-38205	adobe - multiple products	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (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 access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.	2023-09-14	7.5	High
CVE-2023-1108	redhat - multiple products	A flaw was found in undertow. This issue makes achieving a denial of service possible due to an unexpected handshake status updated in SslConduit, where the loop never terminates.	2023-09-14	7.5	High
CVE-2022-3261	redhat - openstack_platform	A flaw was found in OpenStack. Multiple components show plain-text passwords in /var/log/messages during the OpenStack overcloud update run, leading to a disclosure of sensitive information problem.	2023-09-15	7.5	High
CVE-2023-0813	redhat - network_observability	A flaw was found in the Network Observability plugin for OpenShift console. Unless the Loki authToken configuration is set to FORWARD mode, authentication is no longer enforced, allowing any user who can connect to the OpenShift Console in an OpenShift cluster to retrieve flows without authentication.	2023-09-15	7.5	High
CVE-2023-40729	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The affected application lacks security control to prevent unencrypted communication without HTTPS. An attacker who managed to gain machine-in-the-middle position could manipulate, or steal confidential information.	2023-09-12	7.4	High
CVE-2023-42472	sap - businessobjects_business_intelligence_platform	Due to insufficient file type validation, SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface) - version 420, allows a report creator to upload files from local system into the report over the network. When uploading the image file, an authenticated attacker could intercept the request, modify the content type and the extension to read and modify sensitive data causing a high impact on confidentiality and integrity of the application.	2023-09-12	7.3	High
CVE-2023-40724	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). User credentials are found in memory as plaintext. An attacker could perform a memory dump, and get access to credentials, and use it for impersonation.	2023-09-12	7.3	High
CVE-2023-36762	microsoft - multiple products	Microsoft Word Remote Code Execution Vulnerability	2023-09-12	7.3	High
CVE-2023-38743	zohocorp - manageengine_admanager_plus	Zoho ManageEngine ADManager Plus before Build 7200 allows admin users to execute commands on the host machine.	2023-09-11	7.2	High

متاح

CVE-2022-24093	adobe - multiple products	Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability. Exploitation of this issue does not require user interaction and could result in a post-authentication arbitrary code execution.	2023-09-12	7.2	High
CVE-2023-38156	microsoft - azure_hdinsights	Azure HDInsight Apache Ambari Elevation of Privilege Vulnerability	2023-09-12	7.2	High
CVE-2023-23840	solarwinds - orion_platform	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	2023-09-13	7.2	High
CVE-2023-23845	solarwinds - orion_platform	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	2023-09-13	7.2	High
CVE-2023-40623	sap - multiple products	SAP BusinessObjects Suite Installer - version 420, 430, allows an attacker within the network to create a directory under temporary directory and link it to a directory with operating system files. On successful exploitation the attacker can delete all the operating system files causing a limited impact on integrity and completely compromising the availability of the system.	2023-09-12	7.1	High
CVE-2023-4814	trellix - data_loss_prevention	A Privilege escalation vulnerability exists in Trellix Windows DLP endpoint for windows which can be abused to delete any file/folder for which the user does not have permission to.	2023-09-14	7.1	High
CVE-2023-25584	gnu - binutils	An out-of-bounds read flaw was found in the parse_module function in bfd/vms-alpha.c in Binutils.	2023-09-14	7.1	High
CVE-2023-36562	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-09-15	7.1	High
CVE-2023-36805	microsoft - multiple products	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-09-12	7	High
CVE-2023-20135	cisco - multiple products	A vulnerability in Cisco IOS XR Software image verification checks could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system. This vulnerability is due to a time-of-check, time-of-use (TOCTOU) race condition when an install query regarding an ISO image is performed during an install operation that uses an ISO image. An attacker could exploit this vulnerability by modifying an ISO image and then carrying out install requests in parallel. A successful exploit could allow the attacker to execute arbitrary code on an affected device.	2023-09-13	7	High
CVE-2023-36759	microsoft - multiple products	Visual Studio Elevation of Privilege Vulnerability	2023-09-12	6.7	Medium
CVE-2023-39201	zoom - cleanzoom	Untrusted search path in CleanZoom before file date 07/24/2023 may allow a privileged user to conduct an escalation of privilege via local access.	2023-09-12	6.7	Medium
CVE-2023-32461	dell - poweredge_r660_firmware	Dell PowerEdge BIOS and Dell Precision BIOS contain a buffer overflow vulnerability. A local malicious user with high privileges could potentially exploit this vulnerability, leading to corrupt memory and potentially escalate privileges.	2023-09-15	6.7	Medium
CVE-2023-4573	mozilla - multiple products	When receiving rendering data over IPC `mStream` could have been destroyed when initialized, which could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	6.5	Medium
CVE-2023-4574	mozilla - multiple products	When creating a callback over IPC for showing the Color Picker window, multiple of the same callbacks could have been created at a time and eventually all simultaneously destroyed as soon as one of the callbacks finished. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	6.5	Medium
CVE-2023-4575	mozilla - multiple products	When creating a callback over IPC for showing the File Picker window, multiple of the same callbacks could have been created at a time and eventually all simultaneously destroyed as soon as one of the callbacks finished. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	6.5	Medium
CVE-2023-4577	mozilla - multiple products	When `UpdateRegExpStatics` attempted to access `initialStringHeap` it could already have been garbage collected prior to entering the function, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.	2023-09-11	6.5	Medium
CVE-2023-4578	mozilla - multiple products	When calling `JS::CheckRegExpSyntax` a Syntax Error could have been set which would end in calling `convertToRuntimeErrorAndClear`. A path in the function could	2023-09-11	6.5	Medium

متاح

		attempt to allocate memory when none is available which would have caused a newly created Out of Memory exception to be mishandled as a Syntax Error. This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.			
CVE-2023-4580	mozilla - multiple products	Push notifications stored on disk in private browsing mode were not being encrypted potentially allowing the leak of sensitive information. This vulnerability affects Firefox < 117, Firefox ESR < 115.2, and Thunderbird < 115.2.	2023-09-11	6.5	Medium
CVE-2023-40712	apache - airflow	Apache Airflow, versions before 2.7.1, is affected by a vulnerability that allows authenticated users who have access to see the task/dag in the UI, to craft a URL, which could lead to unmasking the secret configuration of the task that otherwise would be masked in the UI. Users are strongly advised to upgrade to version 2.7.1 or later which has removed the vulnerability.	2023-09-12	6.5	Medium
CVE-2023-36799	microsoft - multiple products	.NET Core and Visual Studio Denial of Service Vulnerability	2023-09-12	6.5	Medium
CVE-2023-39215	zoom - multiple products	Improper authentication in Zoom clients may allow an authenticated user to conduct a denial of service via network access.	2023-09-12	6.5	Medium
CVE-2023-25608	fortinet - multiple products	An incomplete filtering of one or more instances of special elements vulnerability [CWE-792] in the command line interpreter of FortiAP-W2 7.2.0 through 7.2.1, 7.0.3 through 7.0.5, 7.0.0 through 7.0.1, 6.4 all versions, 6.2 all versions, 6.0 all versions; FortiAP-C 5.4.0 through 5.4.4, 5.2 all versions; FortiAP 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4 all versions, 6.0 all versions; FortiAP-U 7.0.0, 6.2.0 through 6.2.5, 6.0 all versions, 5.4 all versions may allow an authenticated attacker to read arbitrary files via specially crafted command arguments.	2023-09-13	6.5	Medium
CVE-2023-20233	cisco - multiple products	A vulnerability in the Connectivity Fault Management (CFM) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect processing of invalid continuity check messages (CCMs). An attacker could exploit this vulnerability by sending crafted CCMs to an affected device. A successful exploit could allow the attacker to cause the CFM service to crash when a user displays information about maintenance end points (MEPs) for peer MEPs on an affected device.	2023-09-13	6.5	Medium
CVE-2023-4959	redhat - quay	A flaw was found in Quay. Cross-site request forgery (CSRF) attacks force a user to perform unwanted actions in an application. During the pentest, it was detected that the config-editor page is vulnerable to CSRF. The config-editor page is used to configure the Quay instance. By coercing the victim's browser into sending an attacker-controlled request from another domain, it is possible to reconfigure the Quay instance (including adding users with admin privileges).	2023-09-15	6.5	Medium
CVE-2023-40621	sap - powerdesigner	SAP PowerDesigner Client - version 16.7, allows an unauthenticated attacker to inject VBScript code in a document and have it opened by an unsuspecting user, to have it executed by the application on behalf of the user. The application has a security option to disable or prompt users before untrusted scripts are executed, but this is not set as default.	2023-09-12	6.3	Medium
CVE-2023-29305	adobe - connect	Adobe Connect versions 12.3 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.	2023-09-13	6.1	Medium
CVE-2023-29306	adobe - connect	Adobe Connect versions 12.3 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.	2023-09-13	6.1	Medium
CVE-2023-36727	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-09-15	6.1	Medium
CVE-2023-4813	gnu - glibc	A flaw was found in glibc. In an uncommon situation, the gaih_inet function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the getaddrinfo function is called and the hosts database in /etc/nsswitch.conf is configured with SUCCESS=continue or SUCCESS=merge.	2023-09-12	5.9	Medium
CVE-2023-36777	microsoft - multiple products	Microsoft Exchange Server Information Disclosure Vulnerability	2023-09-12	5.7	Medium
CVE-2023-4155	linux - linux_kernel	A flaw was found in KVM AMD Secure Encrypted Virtualization (SEV) in the Linux kernel. A KVM guest using SEV-ES or SEV-SNP	2023-09-13	5.6	Medium

		with multiple vCPUs can trigger a double fetch race condition vulnerability and invoke the `VMGEXIT` handler recursively. If an attacker manages to call the handler multiple times, they can trigger a stack overflow and cause a denial of service or potentially guest-to-host escape in kernel configurations without stack guard pages (`CONFIG_VMAP_STACK`).			
CVE-2023-4104	mozilla - vpn	An invalid Polkit Authentication check and missing authentication requirements for D-Bus methods allowed any local user to configure arbitrary VPN setups. *This bug only affects Mozilla VPN on Linux. Other operating systems are unaffected.* This vulnerability affects Mozilla VPN client for Linux < v2.16.1.	2023-09-11	5.5	Medium
CVE-2019-7819	adobe - multiple products	Adobe Acrobat Reader versions 2019.010.20098 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	5.5	Medium
CVE-2022-34238	adobe - multiple products	Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 20.005.30334 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-11	5.5	Medium
CVE-2023-35664	google - multiple products	In convertSubgraphFromHAL of ShimConverter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35671	google - multiple products	In onHostEmulationData of HostEmulationManager.java, there is a possible way for a general purpose NFC reader to read the full card number and expiry details when the device is in locked screen mode due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35675	google - multiple products	In loadMediaResumptionControls of MediaResumeListener.kt, there is a possible way to play and listen to media files played by another user on the same device due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35677	google - multiple products	In onCreate of DeviceAdminAdd.java, there is a possible way to forcibly add a device admin due to a missing permission check. This could lead to local denial of service (factory reset or continuous locking) with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35679	google - multiple products	In MtpPropertyValue of MtpProperty.h, there is a possible out of bounds read due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35680	google - multiple products	In multiple locations, there is a possible way to import contacts belonging to other users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-35683	google - multiple products	In bindSelection of DatabaseUtils.java, there is a possible way to access files from other applications due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-09-11	5.5	Medium
CVE-2023-36766	microsoft - multiple products	Microsoft Excel Information Disclosure Vulnerability	2023-09-12	5.5	Medium
CVE-2023-36803	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2023-09-12	5.5	Medium
CVE-2023-38140	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2023-09-12	5.5	Medium
CVE-2023-38160	microsoft - multiple products	Windows TCP/IP Information Disclosure Vulnerability	2023-09-12	5.5	Medium
CVE-2023-41764	microsoft - multiple products	Microsoft Office Spoofing Vulnerability	2023-09-12	5.5	Medium
CVE-2023-40715	fortinet - fortitester	A cleartext storage of sensitive information vulnerability [CWE-312] in FortiTester 2.3.0 through 7.2.3 may allow an attacker with access to the DB contents to retrieve the plaintext password of external servers configured in the device.	2023-09-13	5.5	Medium
CVE-2023-3280	paloaltonetworks - multiple products	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to disable the agent.	2023-09-13	5.5	Medium
CVE-2023-42503	apache - commons_compress	Improper Input Validation, Uncontrolled Resource Consumption vulnerability in Apache Commons Compress in TAR parsing.This issue affects Apache Commons Compress: from 1.22 before 1.24.0.	2023-09-14	5.5	Medium

		Users are recommended to upgrade to version 1.24.0, which fixes the issue. A third party can create a malformed TAR file by manipulating file modification times headers, which when parsed with Apache Commons Compress, will cause a denial of service issue via CPU consumption. In version 1.22 of Apache Commons Compress, support was added for file modification times with higher precision (issue # COMPRESS-612 [1]). The format for the PAX extended headers carrying this data consists of two numbers separated by a period [2], indicating seconds and subsecond precision (for example “1647221103.5998539”). The impacted fields are “atime”, “ctime”, “mtime” and “LIBARCHIVE.creationtime”. No input validation is performed prior to the parsing of header values. Parsing of these numbers uses the BigDecimal [3] class from the JDK which has a publicly known algorithmic complexity issue when doing operations on large numbers, causing denial of service (see issue # JDK-6560193 [4]). A third party can manipulate file time headers in a TAR file by placing a number with a very long fraction (300,000 digits) or a number with exponent notation (such as “9e9999999”) within a file modification time header, and the parsing of files with these headers will take hours instead of seconds, leading to a denial of service via exhaustion of CPU resources. This issue is similar to CVE-2012-2098 [5]. [1]: https://issues.apache.org/jira/browse/COMPRESS-612 [2]: https://pubs.opengroup.org/onlinepubs/9699919799/utilities/pax.html#tag_20_92_13_05 [3]: https://docs.oracle.com/javase/8/docs/api/java/math/BigDecimal.html [4]: https://bugs.openjdk.org/browse/JDK-6560193 [5]: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2098 Only applications using CompressorStreamFactory class (with auto-detection of file types), TarArchiveInputStream and TarFile classes to parse TAR files are impacted. Since this code was introduced in v1.22, only that version and later versions are impacted.			
CVE-2023-38558	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo (Administration Console) V4.0 (All versions), SIMATIC PCS neo (Administration Console) V4.0 Update 1 (All versions). The affected application leaks Windows admin credentials. An attacker with local access to the Administration Console could get the credentials, and impersonate the admin user, thereby gaining admin access to other Windows systems.	2023-09-14	5.5	Medium
CVE-2023-25585	gnu - binutils	A flaw was found in Binutils. The use of an uninitialized field in the struct module *module may lead to application crash and local denial of service.	2023-09-14	5.5	Medium
CVE-2023-25586	gnu - binutils	A flaw was found in Binutils. A logic fail in the bfd_init_section_decompress_status function may lead to the use of an uninitialized variable that can cause a crash and local denial of service.	2023-09-14	5.5	Medium
CVE-2023-25588	gnu - binutils	A flaw was found in Binutils. The field `the_bfd` of `asymbol`struct is uninitialized in the `bfd_mach_o_get_synthetic_symtab` function, which may lead to an application crash and local denial of service.	2023-09-14	5.5	Medium
CVE-2023-40624	sap - multiple products	SAP NetWeaver AS ABAP (applications based on Unified Rendering) - versions SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702, SAP_BASIS 731, allows an attacker to inject JavaScript code that can be executed in the web-application. An attacker could thereby control the behavior of this web-application.	2023-09-12	5.4	Medium
CVE-2023-40625	sap - multiple products	S4CORE (Manage Purchase Contracts App) - versions 102, 103, 104, 105, 106, 107, does not perform necessary authorization checks for an authenticated user. This could allow an attacker to perform unintended actions resulting in escalation of privileges which has low impact on confidentiality and integrity with no impact on availibility of the system.	2023-09-12	5.4	Medium
CVE-2023-0119	redhat - satellite	A stored Cross-site scripting vulnerability was found in foreman. The Comment section in the Hosts tab has incorrect filtering of user input data. As a result of the attack, an attacker with an existing account on the system can steal another user's session, make requests on behalf of the user, and obtain user credentials.	2023-09-12	5.4	Medium

متاح

CVE-2023-36800	microsoft - dynamics_365	Dynamics Finance and Operations Cross-site Scripting Vulnerability	2023-09-12	5.4	Medium
CVE-2023-36886	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-09-12	5.4	Medium
CVE-2023-38164	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-09-12	5.4	Medium
CVE-2023-29183	fortinet - multiple products	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 and FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14 GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management setting.	2023-09-13	5.4	Medium
CVE-2023-38214	adobe - experience_manager	Adobe Experience Manager versions 6.5.17 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-09-13	5.4	Medium
CVE-2023-38215	adobe - multiple products	Adobe Experience Manager versions 6.5.17 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-09-13	5.4	Medium
CVE-2023-37489	sap - businessobjects_business_intelligence	Due to the lack of validation, SAP BusinessObjects Business Intelligence Platform (Version Management System) - version 403, permits an unauthenticated user to read the code snippet through the UI, which leads to low impact on confidentiality and no impact on the application's availability or integrity.	2023-09-12	5.3	Medium
CVE-2023-41367	sap - netweaver	Due to missing authentication check in webdynpro application, an unauthorized user in SAP NetWeaver (Guided Procedures) - version 7.50, can gain access to admin view of specific function anonymously. On successful exploitation of vulnerability under specific circumstances, attacker can view user’s email address. There is no integrity/availability impact.	2023-09-12	5.3	Medium
CVE-2023-41368	sap - multiple products	The OData service of the S4 HANA (Manage checkbook apps) - versions 102, 103, 104, 105, 106, 107, allows an attacker to change the checkbook name by simulating an update OData call.	2023-09-12	5.3	Medium
CVE-2023-36761	microsoft - multiple products	Microsoft Word Information Disclosure Vulnerability	2023-09-12	5.3	Medium
CVE-2023-36801	microsoft - multiple products	DHCP Server Service Information Disclosure Vulnerability	2023-09-12	5.3	Medium
CVE-2023-38152	microsoft - multiple products	DHCP Server Service Information Disclosure Vulnerability	2023-09-12	5.3	Medium
CVE-2021-44172	fortinet - multiple products	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiClientEMS versions 7.0.0 through 7.0.4, 7.0.6 through 7.0.7, in all 6.4 and 6.2 version management interface may allow an unauthenticated attacker to gain information on environment variables such as the EMS installation path.	2023-09-13	5.3	Medium
CVE-2023-27998	fortinet - multiple products	A lack of custom error pages vulnerability [CWE-756] in FortiPresence versions 1.2.0 through 1.2.1 and all versions of 1.1 and 1.0 may allow an unauthenticated attacker with the ability to navigate to the login GUI to gain sensitive information via navigating to specific HTTP(s) paths.	2023-09-13	5.3	Medium
CVE-2023-36551	fortinet - fortisiem	A exposure of sensitive information to an unauthorized actor in Fortinet FortiSIEM version 6.7.0 through 6.7.5 allows attacker to information disclosure via a crafted http request.	2023-09-13	5.3	Medium
CVE-2023-20190	cisco - multiple products	A vulnerability in the classic access control list (ACL) compression feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass the protection that is offered by a configured ACL on an affected device. This vulnerability is due to incorrect destination address range encoding in the compression module of an ACL that is applied to an interface of an affected device. An attacker could exploit this vulnerability by sending traffic through the affected device that should be denied by the configured ACL. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device, allowing the attacker to access trusted networks that the device might be protecting. There are workarounds that address this vulnerability.	2023-09-13	5.3	Medium

		This advisory is part of the September 2023 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: September 2023 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication .			
CVE-2023-38206	adobe - multiple products	Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (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 access the administration CFM and CFC endpoints resulting in a low-confidentiality impact. Exploitation of this issue does not require user interaction.	2023-09-14	5.3	Medium
CVE-2023-4039	gnu - gcc	A failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity.	2023-09-13	4.8	Medium
CVE-2023-4802	proofpoint - insider_threat_management	A reflected cross-site scripting vulnerability in the UpdateInstalledSoftware endpoint of the Insider Threat Management (ITM) Server's web console could be used by an authenticated administrator to run arbitrary javascript within another web console administrator's browser. All versions prior to 7.14.3.69 are affected.	2023-09-13	4.8	Medium
CVE-2023-4803	proofpoint - insider_threat_management	A reflected cross-site scripting vulnerability in the WriteWindowTitle endpoint of the Insider Threat Management (ITM) Server's web console could be used by an authenticated administrator to run arbitrary javascript within another web console administrator's browser. All versions prior to 7.14.3.69 are affected.	2023-09-13	4.8	Medium
CVE-2023-36736	microsoft - identity_linux_broker	Microsoft Identity Linux Broker Remote Code Execution Vulnerability	2023-09-12	4.4	Medium
CVE-2023-4581	mozilla - multiple products	Excel `.xll` add-in files did not have a blocklist entry in Firefox's executable blocklist which allowed them to be downloaded without any warning of their potential harm. This vulnerability affects Firefox < 117, Firefox ESR < 102.15, Firefox ESR < 115.2, Thunderbird < 102.15, and Thunderbird < 115.2.	2023-09-11	4.3	Medium
CVE-2023-41369	sap - multiple products	The Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, 107, 108, allows an attacker to upload the XML file as an attachment. When clicked on the XML file in the attachment section, the file gets opened in the browser to cause the entity loops to slow down the browser.	2023-09-12	4.3	Medium
CVE-2023-40611	apache - airflow	Apache Airflow, versions before 2.7.1, is affected by a vulnerability that allows authenticated and DAG-view authorized Users to modify some DAG run detail values when submitting notes. This could have them alter details such as configuration parameters, start date, etc. Users should upgrade to version 2.7.1 or later which has removed the vulnerability.	2023-09-12	4.3	Medium
CVE-2023-36767	microsoft - multiple products	Microsoft Office Security Feature Bypass Vulnerability	2023-09-12	4.3	Medium
CVE-2023-4900	google - chrome	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to obfuscate a permission prompt via a crafted HTML page. (Chromium security severity: Medium)	2023-09-12	4.3	Medium
CVE-2023-4901	google - chrome	Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially spoof	2023-09-12	4.3	Medium

		security UI via a crafted HTML page. (Chromium security severity: Medium)			
CVE-2023-4902	google - chrome	Inappropriate implementation in Input in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-09-12	4.3	Medium
CVE-2023-4903	google - chrome	Inappropriate implementation in Custom Mobile Tabs in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-09-12	4.3	Medium
CVE-2023-4904	google - chrome	Insufficient policy enforcement in Downloads in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to bypass Enterprise policy restrictions via a crafted download. (Chromium security severity: Medium)	2023-09-12	4.3	Medium
CVE-2023-4905	google - chrome	Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-09-12	4.3	Medium
CVE-2023-4906	google - chrome	Insufficient policy enforcement in Autofill in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low)	2023-09-12	4.3	Medium
CVE-2023-4907	google - chrome	Inappropriate implementation in Intents in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low)	2023-09-12	4.3	Medium
CVE-2023-4908	google - chrome	Inappropriate implementation in Picture in Picture in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low)	2023-09-12	4.3	Medium
CVE-2023-4909	google - chrome	Inappropriate implementation in Interstitials in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low)	2023-09-12	4.3	Medium
CVE-2023-36638	fortinet - multiple products	An improper privilege management vulnerability [CWE-269] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions API may allow a remote and authenticated API admin user to access some system settings such as the mail server settings through the API via a stolen GUI session ID.	2023-09-13	4.3	Medium
CVE-2023-39285	mitel - mivoice_connect	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 SP3 (22.24.5800.0) could allow an unauthenticated attacker to perform a Cross Site Request Forgery (CSRF) attack due to insufficient request validation. A successful exploit could allow an attacker to provide a modified URL, potentially enabling them to modify system configuration settings.	2023-09-14	4.3	Medium
CVE-2023-39286	mitel - connect_mobility_router	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2304.102 could allow an unauthenticated attacker to perform a Cross Site Request Forgery (CSRF) attack due to insufficient request validation. A successful exploit could allow an attacker to provide a modified URL, potentially enabling them to modify system configuration settings.	2023-09-14	4.3	Medium
CVE-2022-20917	cisco - multiple products	A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) message processing feature of Cisco Jabber could allow an authenticated, remote attacker to manipulate the content of XMPP messages that are used by the affected application. This vulnerability is due to the improper handling of nested XMPP messages within requests that are sent to the Cisco Jabber client software. An attacker could exploit this vulnerability by connecting to an XMPP messaging server and sending crafted XMPP messages to an affected Jabber client. A successful exploit could allow the attacker to manipulate the content of XMPP messages, possibly allowing the attacker to cause the Jabber client application to perform unsafe actions.	2023-09-15	4.3	Medium
CVE-2023-4828	proofpoint - insider_threat_management	An improper check for an exceptional condition in the Insider Threat Management (ITM) Server could be used by an attacker to change the configuration of any already-registered agent so that all future agent communications are sent to an attacker-chosen URL. An attacker must first successfully obtain valid agent credentials and target agent hostname. All versions prior to 7.14.3.69 are affected.	2023-09-13	4.2	Medium
CVE-2023-40725	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The affected application returns inconsistent error messages in response to invalid user credentials during login session. This allows an attacker to enumerate usernames, and identify valid usernames.	2023-09-12	4	Medium
CVE-2023-40732	siemens - qms_automotive	A vulnerability has been identified in QMS Automotive (All versions < V12.39). The QMS.Mobile module of the affected	2023-09-12	3.9	Low

		application does not invalidate the session token on logout. This could allow an attacker to perform session hijacking attacks.			
CVE-2023-40442	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8. An app may be able to read sensitive location information.	2023-09-12	3.3	Low
CVE-2023-40218	samsung - exynos_9820_firmware	An issue was discovered in the NPU kernel driver in Samsung Exynos Mobile Processor 9820, 980, 2100, 2200, 1280, and 1380. An integer overflow can bypass detection of error cases via a crafted application.	2023-09-12	3.3	Low
CVE-2023-4579	mozilla - firefox	Search queries in the default search engine could appear to have been the currently navigated URL if the search query itself was a well formed URL. This could have led to a site spoofing another if it had been maliciously set as the default search engine. This vulnerability affects Firefox < 117.	2023-09-11	3.1	Low

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

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