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 12 نوفمبر إلى ١٨ نوفمبر. 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 12th of November to 18th of November. 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-2023-43504	siemens - comos	A vulnerability has been identified in COMOS (All versions < V10.4.4). Ptmcast executable used for testing cache validation service in affected application is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition.	2023-11-14	9.8	Critical
CVE-2023-34991	fortinet - multiple products	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 and 8.4.0 through 8.4.2 and 8.3.0 through 8.3.2 and 8.2.2 allows attacker to execute unauthorized code or commands via a crafted http request.	2023-11-14	9.8	Critical
CVE-2023-36018	microsoft - jupyter	Visual Studio Code Jupyter Extension Spoofing Vulnerability	2023-11-14	9.8	Critical
CVE-2023-36028	microsoft - multiple products	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	2023-11-14	9.8	Critical
CVE-2023-36397	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-11-14	9.8	Critical
CVE-2023-36553	fortinet - multiple products	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 5.4.0 and 5.3.0 through 5.3.3 and 5.2.5 through 5.2.8 and 5.2.1 through 5.2.2 and 5.1.0 through 5.1.3 and 5.0.0 through 5.0.1 and 4.10.0 and 4.9.0 and 4.7.2 allows attacker to execute unauthorized code or commands via crafted API requests.	2023-11-14	9.8	Critical
CVE-2023-31273	intel - data_center_manager	Protection mechanism failure in some Intel DCM software before version 5.2 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2023-11-14	9.8	Critical
CVE-2023-34060	vmware - cloud_director	VMware Cloud Director Appliance contains an authentication bypass vulnerability in case VMware Cloud Director Appliance was upgraded to 10.5 from an older version. On an upgraded version of VMware Cloud Director Appliance 10.5, a malicious actor with network access to the appliance can bypass login restrictions when authenticating on port 22 (ssh) or port 5480 (appliance management console) . This bypass is not present on port 443 (VCD provider and tenant login). On a new installation of VMware Cloud Director Appliance 10.5, the bypass is not present. VMware Cloud Director Appliance is impacted since it uses an affected version of sssd from the underlying Photon OS. The sssd issue is no longer present in versions of Photon OS that ship with sssd-2.8.1-11 or higher (Photon OS 3) or sssd-2.8.2-9 or higher (Photon OS 4 and 5).	2023-11-14	9.8	Critical
CVE-2023-36049	microsoft - .net_framework	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	2023-11-14	9.8	Critical
CVE-2023-45614	arubanetworks - multiple products	There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute	2023-11-14	9.8	Critical

		arbitrary code as a privileged user on the underlying operating system.			
CVE-2023-45615	arubanetworks - multiple products	There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-11-14	9.8	Critical
CVE-2023-45616	arubanetworks - multiple products	There is a buffer overflow vulnerability in the underlying AirWave client service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-11-14	9.8	Critical
CVE-2023-39335	ivanti - multiple products	A security vulnerability has been identified in EPMM Versions 11.10, 11.9 and 11.8 and older allowing an unauthenticated threat actor to impersonate any existing user during the device enrollment process. This issue poses a significant security risk, as it enables unauthorized access and potential misuse of user accounts and resources.	2023-11-15	9.8	Critical
CVE-2023-47003	redislabs - redisgraph	An issue in RedisGraph v.2.12.10 allows an attacker to execute arbitrary code and cause a denial of service via a crafted string in DataBlock_ItemIsDeleted.	2023-11-16	9.8	Critical
CVE-2023-44324	adobe - framemaker	Adobe FrameMaker versions 2022 and earlier are affected by an Improper Authentication vulnerability that could result in a Security feature bypass. An unauthenticated attacker can abuse this vulnerability to access the API and leak default admin's password. Exploitation of this issue does not require user interaction.	2023-11-17	9.8	Critical
CVE-2023-44350	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	2023-11-17	9.8	Critical
CVE-2023-44351	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	2023-11-17	9.8	Critical
CVE-2023-44353	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	2023-11-17	9.8	Critical
CVE-2023-25603	fortinet - multiple products	A permissive cross-domain policy with untrusted domains vulnerability in Fortinet FortiADC 7.1.0 - 7.1.1, FortiDDoS-F 6.3.0 - 6.3.4 and 6.4.0 - 6.4.1 allow an unauthorized attacker to carry out privileged actions and retrieve sensitive information via crafted web requests.	2023-11-14	9.1	Critical
CVE-2023-39337	ivanti - multiple products	A security vulnerability in EPMM Versions 11.10, 11.9 and 11.8 older allows a threat actor with knowledge of an enrolled device identifier to access and extract sensitive information, including device and environment configuration details, as well as secrets. This vulnerability poses a serious security risk, potentially exposing confidential data and system integrity.	2023-11-15	9.1	Critical
CVE-2023-46098	siemens - simatic_pcs_neo	A vulnerability has been identified in SIMATIC PCS neo (All versions < V4.1). When accessing the Information Server from affected products, the products use an overly permissive CORS policy. This could allow an attacker to trick a legitimate user to trigger unwanted behavior.	2023-11-14	8.8	High
CVE-2023-26205	fortinet - multiple products	An improper access control vulnerability [CWE-284] in FortiADC automation feature 7.1.0 through 7.1.2, 7.0 all versions, 6.2 all versions, 6.1 all versions may allow an authenticated low-privileged attacker to escalate their privileges to super_admin via a specific crafted configuration of fabric automation CLI script.	2023-11-14	8.8	High
CVE-2023-36017	microsoft - multiple products	Windows Scripting Engine Memory Corruption Vulnerability	2023-11-14	8.8	High
CVE-2023-36025	microsoft - multiple products	Windows SmartScreen Security Feature Bypass Vulnerability	2023-11-14	8.8	High
CVE-2023-36400	microsoft - multiple products	Windows HMAC Key Derivation Elevation of Privilege Vulnerability	2023-11-14	8.8	High
CVE-2023-36402	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-11-14	8.8	High
CVE-2023-36423	microsoft - multiple products	Microsoft Remote Registry Service Remote Code Execution Vulnerability	2023-11-14	8.8	High
CVE-2023-36560	microsoft - .net_framework	ASP.NET Security Feature Bypass Vulnerability	2023-11-14	8.8	High
CVE-2023-38151	microsoft - multiple products	Microsoft Host Integration Server 2020 Remote Code Execution Vulnerability	2023-11-14	8.8	High

CVE-2023-22663	intel - unison_software	Improper authentication for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-11-14	8.8	High
CVE-2023-32641	intel - quickassist_technology	Improper input validation in firmware for Intel(R) QAT before version QAT20.L.1.0.40-00004 may allow escalation of privilege and denial of service via adjacent access.	2023-11-14	8.8	High
CVE-2023-36860	intel - unison_software	Improper input validation for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-11-14	8.8	High
CVE-2023-39221	intel - unison_software	Improper access control for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-11-14	8.8	High
CVE-2023-39412	intel - unison_software	Cross-site request forgery in some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-11-14	8.8	High
CVE-2023-36437	microsoft - azure_pipelines_agent	Azure DevOps Server Remote Code Execution Vulnerability	2023-11-14	8.8	High
CVE-2023-43582	zoom - multiple products	Improper authorization in some Zoom clients may allow an authorized user to conduct an escalation of privilege via network access.	2023-11-15	8.8	High
CVE-2023-5997	google - chrome	Use after free in Garbage Collection in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-15	8.8	High
CVE-2023-6112	google - chrome	Use after free in Navigation in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-15	8.8	High
CVE-2023-36052	microsoft - azure_cli	Azure CLI REST Command Information Disclosure Vulnerability	2023-11-14	8.6	High
CVE-2023-45617	arubanetworks - multiple products	There are arbitrary file deletion vulnerabilities in the CLI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.	2023-11-14	8.2	High
CVE-2023-45618	arubanetworks - multiple products	There are arbitrary file deletion vulnerabilities in the AirWave client service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.	2023-11-14	8.2	High
CVE-2023-45619	arubanetworks - multiple products	There is an arbitrary file deletion vulnerability in the RSSI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of this vulnerability results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.	2023-11-14	8.2	High
CVE-2023-45794	siemens - multiple products	A vulnerability has been identified in Mendix Applications using Mendix 10 (All versions < V10.4.0), Mendix Applications using Mendix 7 (All versions < V7.23.37), Mendix Applications using Mendix 8 (All versions < V8.18.27), Mendix Applications using Mendix 9 (All versions < V9.24.10). A capture-replay flaw in the platform could have an impact to apps built with the platform, if certain preconditions are met that depend on the app's model and access control design. This could allow authenticated attackers to access or modify objects without proper authorization, or escalate privileges in the context of the vulnerable app.	2023-11-14	8.1	High
CVE-2023-31403	sap - business_one	SAP Business One installation - version 10.0, does not perform proper authentication and authorization checks for SMB shared folder. As a result, any malicious user can read and write to the SMB shared folder. Additionally, the files in the folder can be executed or be used by the installation process leading to considerable impact on confidentiality, integrity and availability.	2023-11-14	8	High
CVE-2023-46097	siemens - simatic_pcs_neo	A vulnerability has been identified in SIMATIC PCS neo (All versions < V4.1). The PUD Manager of affected products does not properly neutralize user provided inputs. This could allow an authenticated adjacent attacker to execute SQL statements in the underlying database.	2023-11-14	8	High
CVE-2023-36021	microsoft - on-prem_data_gateway	Microsoft On-Prem Data Gateway Security Feature Bypass Vulnerability	2023-11-14	8	High
CVE-2023-36035	microsoft - multiple products	Microsoft Exchange Server Spoofing Vulnerability	2023-11-14	8	High
CVE-2023-36039	microsoft - multiple products	Microsoft Exchange Server Spoofing Vulnerability	2023-11-14	8	High

CVE-2023-36050	microsoft - multiple products	Microsoft Exchange Server Spoofing Vulnerability	2023-11-14	8	High
CVE-2023-36425	microsoft - multiple products	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	2023-11-14	8	High
CVE-2023-36439	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-11-14	8	High
CVE-2023-6111	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_trans_gc_catchall did not remove the catchall set element from the catchall_list when the argument sync is true, making it possible to free a catchall set element many times. We recommend upgrading past commit 93995bf4af2c5a99e2a87f0cd5ce547d31eb7630.	2023-11-14	7.8	High
CVE-2023-36033	microsoft - multiple products	Windows DWM Core Library Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36036	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36037	microsoft - multiple products	Microsoft Excel Security Feature Bypass Vulnerability	2023-11-14	7.8	High
CVE-2023-36041	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-11-14	7.8	High
CVE-2023-36045	microsoft - multiple products	Microsoft Office Graphics Remote Code Execution Vulnerability	2023-11-14	7.8	High
CVE-2023-36047	microsoft - multiple products	Windows Authentication Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36393	microsoft - multiple products	Windows User Interface Application Core Remote Code Execution Vulnerability	2023-11-14	7.8	High
CVE-2023-36396	microsoft - multiple products	Windows Compressed Folder Remote Code Execution Vulnerability	2023-11-14	7.8	High
CVE-2023-36407	microsoft - multiple products	Windows Hyper-V Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36408	microsoft - multiple products	Windows Hyper-V Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36422	microsoft - windows_defender	Microsoft Windows Defender Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36424	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36705	microsoft - multiple products	Windows Installer Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-36719	microsoft - multiple products	Microsoft Speech Application Programming Interface (SAPI) Elevation of Privilege Vulnerability	2023-11-14	7.8	High
CVE-2023-41840	fortinet - multiple products	A untrusted search path vulnerability in Fortinet FortiClientWindows 7.0.9 allows an attacker to perform a DLL Hijack attack via a malicious OpenSSL engine library in the search path.	2023-11-14	7.8	High
CVE-2022-27229	intel - hdmi_firmware	Path transversal in some Intel(R) NUC Kits NUC7i3DN, NUC7i5DN, NUC7i7DN HDMI firmware update tool software before version 1.79.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2022-33898	intel - nuc_watchdog_timer_utility	Insecure inherited permissions in some Intel(R) NUC Watchdog Timer installation software before version 2.0.21.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2022-38786	intel - battery_life_diagnostic_tool	Improper access control in some Intel Battery Life Diagnostic Tool software before version 2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2022-41689	intel - in-band_manageability	Improper access control in some Intel In-Band Manageability software before version 3.0.14 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2022-41700	intel - nuc_pro_software_suite	Insecure inherited permissions in some Intel(R) NUC Pro Software Suite installation software before version 2.0.0.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2022-45469	intel - unison_software	Improper input validation for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-22292	intel - unison_software	Uncaught exception for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-28377	intel - usb_firmware	Improper authentication in some Intel(R) NUC Kit NUC11PH USB firmware installation software before version 1.1 for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-28397	intel - aptio_v_uefi_firmware_integrator_tools	Improper access control in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated to potentially enable escalation of privileges via local access.	2023-11-14	7.8	High

CVE-2023-28737	intel - aptio_v_uefi_firmware_integrator_tools	Improper initialization in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-29157	intel - one_boot_flash_update	Improper access control in some Intel(R) OFU software before version 14.1.31 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-29161	intel - one_boot_flash_update	Uncontrolled search path in some Intel(R) OFU software before version 14.1.31 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-29504	intel - realsense_d400_series_dynamic_calibration_tool	Uncontrolled search path element in some Intel(R) RealSense(TM) Dynamic Calibration software before version 2.13.1.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-32204	intel - one_boot_flash_update	Improper access control in some Intel(R) OFU software before version 14.1.31 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-32638	intel - arc_rgb_controller	Incorrect default permissions in some Intel Arc RGB Controller software before version 1.06 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-32661	intel - realtek_sd_card_reader_driver	Improper authentication in some Intel(R) NUC Kits NUC7PJYH and NUC7CJYH Realtek* SD Card Reader Driver installation software before version 10.0.19041.29098 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-33878	intel - audio_install_package	Path transversal in some Intel(R) NUC P14E Laptop Element Audio Install Package software before version 156 for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-34314	intel - simics_simulator	Insecure inherited permissions in some Intel(R) Simics Simulator software before version 1.7.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-34350	intel - extreme_tuning_utility	Uncontrolled search path element in some Intel(R) XTU software before version 7.12.0.15 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-34430	intel - battery_life_diagnostic_tool	Uncontrolled search path in some Intel Battery Life Diagnostic Tool software before version 2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-34997	intel - server_configuration_utility	Insecure inherited permissions in the installer for some Intel Server Configuration Utility software before version 16.0.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-38411	intel - smart_campus	Improper access control in the Intel Smart Campus android application before version 9.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-38570	intel - unison_software	Access of memory location after end of buffer for some Intel Unison software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-39230	intel - rapid_storage_technology	Insecure inherited permissions in some Intel Rapid Storage Technology software before version 16.8.5.1014.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.8	High
CVE-2023-35080	ivanti - multiple products	A vulnerability has been identified in the Ivanti Secure Access Windows client, which could allow a locally authenticated attacker to exploit a vulnerable configuration, potentially leading to various security risks, including the escalation of privileges, denial of service, or information disclosure.	2023-11-15	7.8	High
CVE-2023-38043	ivanti - multiple products	A vulnerability exists on all versions of the Ivanti Secure Access Client below 22.6R1.1, which could allow a locally authenticated attacker to exploit a vulnerable configuration, potentially leading to a denial of service (DoS) condition on the user machine and, in some cases, resulting in a full compromise of the system.	2023-11-15	7.8	High
CVE-2023-38543	ivanti - multiple products	A vulnerability exists on all versions of the Ivanti Secure Access Client below 22.6R1.1, which could allow a locally authenticated attacker to exploit a vulnerable configuration, potentially leading to a denial of service (DoS) condition on the user machine.	2023-11-15	7.8	High
CVE-2023-41718	ivanti - multiple products	When a particular process flow is initiated, an attacker may be able to gain unauthorized elevated privileges on the affected system when having control over a specific file.	2023-11-15	7.8	High
CVE-2023-43590	zoom - rooms	Link following in Zoom Rooms for macOS before version 5.16.0 may allow an authenticated user to conduct an escalation of privilege via local access.	2023-11-15	7.8	High
CVE-2023-43591	zoom - rooms	Improper privilege management in Zoom Rooms for macOS before version 5.16.0 may allow an authenticated user to conduct an escalation of privilege via local access.	2023-11-15	7.8	High
CVE-2023-39259	dell - multiple products	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system.	2023-11-16	7.8	High

CVE-2023-44282	dell - repository_manager	Dell Repository Manager, 3.4.3 and prior, contains an Improper Access Control vulnerability in its installation module. A local low-privileged attacker could potentially exploit this vulnerability, leading to gaining escalated privileges.	2023-11-16	7.8	High
CVE-2023-44292	dell - repository_manager	Dell Repository Manager, 3.4.3 and prior, contains an Improper Access Control vulnerability in its installation module. A local low-privileged attacker could potentially exploit this vulnerability, leading to gaining escalated privileges.	2023-11-16	7.8	High
CVE-2023-44336	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44337	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44338	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44359	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44365	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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.	2023-11-16	7.8	High
CVE-2023-44366	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44367	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44371	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44372	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	7.8	High
CVE-2023-44330	adobe - photoshop	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (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.	2023-11-16	7.8	High
CVE-2023-47040	adobe - multiple products	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-47041	adobe - multiple products	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-47042	adobe - multiple products	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability	2023-11-16	7.8	High

		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.			
CVE-2023-47043	adobe - multiple products	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-26368	adobe - multiple products	Adobe InCopy versions 18.5 (and earlier) and 17.4.2 (and earlier) are affected by 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.	2023-11-16	7.8	High
CVE-2023-47046	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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.	2023-11-16	7.8	High
CVE-2023-47047	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer 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.	2023-11-16	7.8	High
CVE-2023-47048	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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.	2023-11-16	7.8	High
CVE-2023-47049	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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.	2023-11-16	7.8	High
CVE-2023-47050	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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.	2023-11-16	7.8	High
CVE-2023-47051	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by a Heap-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.	2023-11-16	7.8	High
CVE-2023-47055	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-47056	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by a Heap-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.	2023-11-16	7.8	High
CVE-2023-47057	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-47058	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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.	2023-11-16	7.8	High
CVE-2023-47059	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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	2023-11-16	7.8	High

		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.			
CVE-2023-6176	linux - linux_kernel	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk functionality. This issue occurs when a user constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system or escalate their privileges on the system.	2023-11-16	7.8	High
CVE-2023-47066	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-47067	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-47068	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-47069	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-47070	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-47073	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	7.8	High
CVE-2023-43503	siemens - comos	A vulnerability has been identified in COMOS (All versions < V10.4.4). Caching system in the affected application leaks sensitive information such as user and project information in cleartext via UDP.	2023-11-14	7.5	High
CVE-2023-46590	siemens - siemens_opc_ua_modeling_editor	A vulnerability has been identified in Siemens OPC UA Modelling Editor (SiOME) (All versions < V2.8). Affected products suffer from a XML external entity (XXE) injection vulnerability. This vulnerability could allow an attacker to interfere with an application's processing of XML data and read arbitrary files in the system.	2023-11-14	7.5	High
CVE-2023-46601	siemens - comos	A vulnerability has been identified in COMOS (All versions). The affected application lacks proper access controls in making the SQLServer connection. This could allow an attacker to query the database directly to access information that the user should not have access to.	2023-11-14	7.5	High
CVE-2023-36392	microsoft - multiple products	DHCP Server Service Denial of Service Vulnerability	2023-11-14	7.5	High
CVE-2023-36395	microsoft - multiple products	Windows Deployment Services Denial of Service Vulnerability	2023-11-14	7.5	High
CVE-2023-42783	fortinet - multiple products	A relative path traversal in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 and 8.4.2 through 8.4.0 and 8.3.2 through 8.3.0 and 8.2.2 allows attacker to read arbitrary files via crafted http requests.	2023-11-14	7.5	High
CVE-2023-22285	intel - unison_software	Improper access control for some Intel Unison software may allow an unauthenticated user to potentially enable denial of service via network access.	2023-11-14	7.5	High
CVE-2023-22337	intel - unison_software	Improper input validation for some Intel Unison software may allow an unauthenticated user to potentially enable denial of service via network access.	2023-11-14	7.5	High
CVE-2023-31203	intel - openvino_model_server	Improper input validation in some OpenVINO Model Server software before version 2022.3 for Intel Distribution of OpenVINO toolkit may allow an unauthenticated user to potentially enable denial of service via network access.	2023-11-14	7.5	High

CVE-2023-32279	intel - connectivity_performance_suite	Improper access control in user mode driver for some Intel(R) Connectivity Performance Suite before version 2.1123.214.2 may allow unauthenticated user to potentially enable information disclosure via network access.	2023-11-14	7.5	High
CVE-2023-39228	intel - unison_software	Improper access control for some Intel Unison software may allow an unauthenticated user to potentially enable denial of service via network access.	2023-11-14	7.5	High
CVE-2023-36038	microsoft - multiple products	ASP.NET Core Denial of Service Vulnerability	2023-11-14	7.5	High
CVE-2023-39203	zoom - multiple products	Uncontrolled resource consumption in Zoom Team Chat for Zoom Desktop Client for Windows and Zoom VDI Client may allow an unauthenticated user to conduct a disclosure of information via network access.	2023-11-14	7.5	High
CVE-2023-39204	zoom - multiple products	Buffer overflow in some Zoom clients may allow an unauthenticated user to conduct a denial of service via network access.	2023-11-14	7.5	High
CVE-2023-39206	zoom - multiple products	Buffer overflow in some Zoom clients may allow an unauthenticated user to conduct a denial of service via network access.	2023-11-14	7.5	High
CVE-2023-45620	arubanetworks - multiple products	Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.	2023-11-14	7.5	High
CVE-2023-45621	arubanetworks - multiple products	Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.	2023-11-14	7.5	High
CVE-2023-45622	arubanetworks - multiple products	Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the BLE daemon service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.	2023-11-14	7.5	High
CVE-2023-45623	arubanetworks - multiple products	Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the Wi-Fi Uplink service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.	2023-11-14	7.5	High
CVE-2023-45624	arubanetworks - multiple products	An unauthenticated Denial-of-Service (DoS) vulnerability exists in the soft ap daemon accessed via the PAPI protocol. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.	2023-11-14	7.5	High
CVE-2023-22272	adobe - robohelp_server	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction.	2023-11-17	7.5	High
CVE-2023-22274	adobe - robohelp_server	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction.	2023-11-17	7.5	High
CVE-2023-22275	adobe - robohelp_server	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction.	2023-11-17	7.5	High
CVE-2023-26347	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.	2023-11-17	7.5	High
CVE-2023-45582	fortinet - multiple products	An improper restriction of excessive authentication attempts vulnerability [CWE-307] in FortiMail webmail version 7.2.0 through 7.2.4, 7.0.0 through 7.0.6 and before 6.4.8 may allow an unauthenticated attacker to perform a brute force attack on the affected endpoints via repeated login attempts.	2023-11-14	7.3	High
CVE-2023-32278	intel - nuc_uniwill_service_driver	Path transversal in some Intel(R) NUC Uniwill Service Driver for Intel(R) NUC M15 Laptop Kits - LAPRC510 & LAPRC710 Uniwill Service Driver installation software before version 1.0.1.7 for Intel(R) NUC Software Studio may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.3	High
CVE-2023-32655	intel - usb_type_c_power_delivery_controller	Path transversal in some Intel(R) NUC Kits & Mini PCs - NUC8i7HVK & NUC8HNK USB Type C power delivery controller installatio software before version 1.0.10.3 for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.3	High
CVE-2023-32658	intel - hdmi_firmware	Unquoted search path in some Intel(R) NUC Kits NUC7i3DN, NUC7i5DN, NUC7i7DN HDMI firmware update tool software before version 1.79.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.3	High

CVE-2023-32660	intel - thunderbolt_3_controller_firmware	Uncontrolled search path in some Intel(R) NUC Kit NUC6i7KYK Thunderbolt(TM) 3 Firmware Update Tool installation software before version 46 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.3	High
CVE-2023-33874	intel - hid_event_filter_driver	Uncontrolled search path in some Intel(R) NUC 12 Pro Kits & Mini PCs - NUC12WS Intel(R) HID Event Filter Driver installation software before version 2.2.2.1 for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-11-14	7.3	High
CVE-2023-44317	siemens - scalance_xb208_\(e\/ip\)_firmware	A vulnerability has been identified in SCALANCE XB205-3 (SC, PN) (All versions < V4.5), SCALANCE XB205-3 (ST, E/IP) (All versions < V4.5), SCALANCE XB205-3 (ST, E/IP) (All versions < V4.5), SCALANCE XB205-3 (ST, PN) (All versions < V4.5), SCALANCE XB205-3LD (SC, E/IP) (All versions < V4.5), SCALANCE XB205-3LD (SC, PN) (All versions < V4.5), SCALANCE XB208 (E/IP) (All versions < V4.5), SCALANCE XB208 (PN) (All versions < V4.5), SCALANCE XB213-3 (SC, E/IP) (All versions < V4.5), SCALANCE XB213-3 (SC, PN) (All versions < V4.5), SCALANCE XB213-3 (ST, E/IP) (All versions < V4.5), SCALANCE XB213-3 (ST, PN) (All versions < V4.5), SCALANCE XB213-3LD (SC, E/IP) (All versions < V4.5), SCALANCE XB213-3LD (SC, PN) (All versions < V4.5), SCALANCE XB216 (E/IP) (All versions < V4.5), SCALANCE XB216 (PN) (All versions < V4.5), SCALANCE XC206-2 (SC) (All versions < V4.5), SCALANCE XC206-2 (ST/BFOC) (All versions < V4.5), SCALANCE XC206-2G PoE (All versions < V4.5), SCALANCE XC206-2G PoE (54 V DC) (All versions < V4.5), SCALANCE XC206-2G PoE EEC (54 V DC) (All versions < V4.5), SCALANCE XC206-2SFP (All versions < V4.5), SCALANCE XC206-2SFP EEC (All versions < V4.5), SCALANCE XC206-2SFP G (All versions < V4.5), SCALANCE XC206-2SFP G (EIP DEF.) (All versions < V4.5), SCALANCE XC206-2SFP G EEC (All versions < V4.5), SCALANCE XC208 (All versions < V4.5), SCALANCE XC208EEC (All versions < V4.5), SCALANCE XC208G (All versions < V4.5), SCALANCE XC208G (EIP def.) (All versions < V4.5), SCALANCE XC208G EEC (All versions < V4.5), SCALANCE XC208G PoE (All versions < V4.5), SCALANCE XC208G PoE (54 V DC) (All versions < V4.5), SCALANCE XC216 (All versions < V4.5), SCALANCE XC216-3G PoE (All versions < V4.5), SCALANCE XC216-3G PoE (54 V DC) (All versions < V4.5), SCALANCE XC216-4C (All versions < V4.5), SCALANCE XC216-4C G (All versions < V4.5), SCALANCE XC216-4C G (EIP Def.) (All versions < V4.5), SCALANCE XC216-4C G EEC (All versions < V4.5), SCALANCE XC216EEC (All versions < V4.5), SCALANCE XC224 (All versions < V4.5), SCALANCE XC224-4C G (All versions < V4.5), SCALANCE XC224-4C G (EIP Def.) (All versions < V4.5), SCALANCE XC224-4C G EEC (All versions < V4.5), SCALANCE XF204 (All versions < V4.5), SCALANCE XF204 DNA (All versions < V4.5), SCALANCE XF204-2BA (All versions < V4.5), SCALANCE XF204-2BA DNA (All versions < V4.5), SCALANCE XP208 (All versions < V4.5), SCALANCE XP208 (Ethernet/IP) (All versions < V4.5), SCALANCE XP208EEC (All versions < V4.5), SCALANCE XP208PoE EEC (All versions < V4.5), SCALANCE XP216 (All versions < V4.5), SCALANCE XP216 (Ethernet/IP) (All versions < V4.5), SCALANCE XP216EEC (All versions < V4.5), SCALANCE XP216POE EEC (All versions < V4.5), SCALANCE XR324WG (24 x FE, AC 230V) (All versions < V4.5), SCALANCE XR324WG (24 X FE, DC 24V) (All versions < V4.5), SCALANCE XR326-2C PoE WG (All versions < V4.5), SCALANCE XR326-2C PoE WG (without UL) (All versions < V4.5), SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (All versions < V4.5), SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (All versions < V4.5), SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (All versions < V4.5), SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (All versions < V4.5), SCALANCE XR328-4C WG (28xGE, AC 230V) (All versions < V4.5), SCALANCE XR328-4C WG (28xGE, DC 24V) (All versions < V4.5), SIPLUS NET SCALANCE XC206-2 (All versions < V4.5), SIPLUS NET SCALANCE XC206-2SFP (All versions < V4.5), SIPLUS NET SCALANCE XC208 (All versions < V4.5), SIPLUS NET SCALANCE XC216-4C (All versions < V4.5). Affected products do not properly validate the content of uploaded X509 certificates which could allow an attacker with administrative privileges to execute arbitrary code on the device.	2023-11-14	7.2	High
CVE-2023-36401	microsoft - multiple products	Microsoft Remote Registry Service Remote Code Execution Vulnerability	2023-11-14	7.2	High
CVE-2023-22448	intel - unison_software	Improper access control for some Intel Unison software may allow a privileged user to potentially enable escalation of privilege via network access.	2023-11-14	7.2	High
CVE-2023-45625	arubanetworks - multiple products	Multiple authenticated command injection vulnerabilities exist in the command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2023-11-14	7.2	High

CVE-2023-45626	arubanetworks - multiple products	An authenticated vulnerability has been identified allowing an attacker to effectively establish highly privileged persistent arbitrary code execution across boot cycles.	2023-11-14	7.2	High
CVE-2023-22273	adobe - robohelp_server	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to Remote Code Execution by an admin authenticated attacker. Exploitation of this issue does not require user interaction.	2023-11-17	7.2	High
CVE-2023-36046	microsoft - multiple products	Windows Authentication Denial of Service Vulnerability	2023-11-14	7.1	High
CVE-2023-36399	microsoft - multiple products	Windows Storage Elevation of Privilege Vulnerability	2023-11-14	7.1	High
CVE-2022-40681	fortinet - multiple products	A incorrect authorization in Fortinet FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to cause denial of service via sending a crafted request to a specific named pipe.	2023-11-14	7.1	High
CVE-2023-36394	microsoft - multiple products	Windows Search Service Elevation of Privilege Vulnerability	2023-11-14	7	High
CVE-2023-36403	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-11-14	7	High
CVE-2023-36405	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-11-14	7	High
CVE-2023-36427	microsoft - multiple products	Windows Hyper-V Elevation of Privilege Vulnerability	2023-11-14	7	High
CVE-2023-38177	microsoft - multiple products	Microsoft SharePoint Server Remote Code Execution Vulnerability	2023-11-14	6.8	Medium
CVE-2023-28002	fortinet - multiple products	An improper validation of integrity check value vulnerability [CWE-354] in FortiOS 7.2.0 through 7.2.3, 7.0.0 through 7.0.12, 6.4 all versions, 6.2 all versions, 6.0 all versions and FortiProxy 7.2 all versions, 7.0 all versions, 2.0 all versions VMs may allow a local attacker with admin privileges to boot a malicious image on the device and bypass the filesystem integrity check in place.	2023-11-14	6.7	Medium
CVE-2022-24379	intel - server_board_m70klp2sb_firmware	Improper input validation in some Intel(R) Server System M70KLP Family BIOS firmware before version 01.04.0029 may allow a privileged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2022-29262	intel - server_board_m70klp2sb_firmware	Improper buffer restrictions in some Intel(R) Server Board BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2022-33945	intel - server_board_m70klp2sb_firmware	Improper input validation in some Intel(R) Server board and Intel(R) Server System BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2022-36374	intel - aptio_v_uefi_firmware_integrator_tools	Improper access control in some Intel(R) Aptio* V UEFI Firmware Integrator Tools before version iDmi Windows 5.27.03.0003 may allow a privileged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2022-36396	intel - aptio_v_uefi_firmware_integrator_tools	Improper access control in some Intel(R) Aptio* V UEFI Firmware Integrator Tools before version iDmiEdit-Linux-5.27.06.0017 may allow a privileged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2023-29177	fortinet - multiple products	Multiple buffer copy without checking size of input ('classic buffer overflow') vulnerabilities [CWE-120] in FortiADC version 7.2.0 and before 7.1.2 & FortiDDoS-F version 6.5.0 and before 6.4.1 allows a privileged attacker to execute arbitrary code or commands via specifically crafted CLI requests.	2023-11-14	6.7	Medium
CVE-2023-32662	intel - battery_life_diagnostic_tool	Improper authorization in some Intel Battery Life Diagnostic Tool installation software before version 2.2.1 may allow a privilaged user to potentially enable escalation of privilege via local access.	2023-11-14	6.7	Medium
CVE-2023-34431	intel - server_board_m70klp2sb_firmware	Improper input validation in some Intel(R) Server Board BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access	2023-11-14	6.7	Medium
CVE-2023-36008	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2023-11-16	6.6	Medium
CVE-2023-42781	apache - airflow	Apache Airflow, versions before 2.7.3, has a vulnerability that allows an authorized user who has access to read specific DAGs only, to read information about task instances in other DAGs. This is a different issue than CVE-2023-42663 but leading to similar outcome. Users of Apache Airflow are advised to upgrade to version 2.7.3 or newer to mitigate the risk associated with this vulnerability.	2023-11-12	6.5	Medium
CVE-2023-43505	siemens - comos	A vulnerability has been identified in COMOS (All versions). The affected application lacks proper access controls in SMB shares. This could allow an attacker to access files that the user should not have access to.	2023-11-14	6.5	Medium
CVE-2023-46096	siemens - simatic_pcs_neo	A vulnerability has been identified in SIMATIC PCS neo (All versions < V4.1). The PUD Manager of affected products does not properly authenticate users in the PUD Manager web service. This could allow an unauthenticated adjacent attacker to generate a privileged token and upload additional documents.	2023-11-14	6.5	Medium

CVE-2023-36043	microsoft - multiple products	Open Management Infrastructure Information Disclosure Vulnerability	2023-11-14	6.5	Medium
CVE-2023-36398	microsoft - multiple products	Windows NTFS Information Disclosure Vulnerability	2023-11-14	6.5	Medium
CVE-2023-36413	microsoft - multiple products	Microsoft Office Security Feature Bypass Vulnerability	2023-11-14	6.5	Medium
CVE-2023-36641	fortinet - multiple products	A numeric truncation error in Fortinet FortiProxy version 7.2.0 through 7.2.4, FortiProxy version 7.0.0 through 7.0.10, FortiProxy 2.0 all versions, FortiProxy 1.2 all versions, FortiProxy 1.1, all versions, FortiProxy 1.0 all versions, FortiOS version 7.4.0, FortiOS version 7.2.0 through 7.2.5, FortiOS version 7.0.0 through 7.0.12, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions allows attacker to denial of service via specifically crafted HTTP requests.	2023-11-14	6.5	Medium
CVE-2023-41676	fortinet - multiple products	An exposure of sensitive information to an unauthorized actor [CWE-200] in FortiSIEM version 7.0.0 and before 6.7.5 may allow an attacker with access to windows agent logs to obtain the windows agent password via searching through the logs.	2023-11-14	6.5	Medium
CVE-2023-22290	intel - unison_software	Uncaught exception for some Intel Unison software may allow an authenticated user to potentially enable denial of service via network access.	2023-11-14	6.5	Medium
CVE-2023-28376	intel - ethernet_network_adapter_e810-2cqda2_firmware	Out-of-bounds read in the firmware for some Intel(R) E810 Ethernet Controllers and Adapters before version 1.7.1 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2023-11-14	6.5	Medium
CVE-2023-38131	intel - unison_software	Improper input validationation for some Intel Unison software may allow an authenticated user to potentially enable denial of service via network access.	2023-11-14	6.5	Medium
CVE-2023-39199	zoom - multiple products	Cryptographic issues with In-Meeting Chat for some Zoom clients may allow a privileged user to conduct an information disclosure via network access.	2023-11-14	6.5	Medium
CVE-2023-39205	zoom - multiple products	Improper conditions check in Zoom Team Chat for Zoom clients may allow an authenticated user to conduct a denial of service via network access.	2023-11-14	6.5	Medium
CVE-2023-45627	arubanetworks - multiple products	An authenticated Denial-of-Service (DoS) vulnerability exists in the CLI service. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.	2023-11-14	6.5	Medium
CVE-2023-5189	redhat - multiple products	A path traversal vulnerability exists in Ansible when extracting tarballs. An attacker could craft a malicious tarball so that when using the galaxy importer of Ansible Automation Hub, a symlink could be dropped on the disk, resulting in files being overwritten.	2023-11-14	6.5	Medium
CVE-2023-43588	zoom - multiple products	Insufficient control flow management in some Zoom clients may allow an authenticated user to conduct an information disclosure via network access.	2023-11-15	6.5	Medium
CVE-2023-22268	adobe - robohelp_server	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an low-privileged authenticated attacker. Exploitation of this issue does not require user interaction.	2023-11-17	6.5	Medium
CVE-2023-38364	ibm - cics_tx	IBM CICS TX Advanced 10.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 260821.	2023-11-13	6.1	Medium
CVE-2023-36030	microsoft - multiple products	Microsoft Dynamics 365 Sales Spoofing Vulnerability	2023-11-14	6.1	Medium
CVE-2023-47797	liferay - liferay_portal	Reflected cross-site scripting (XSS) vulnerability on a content page’s edit page in Liferay Portal 7.4.3.94 through 7.4.3.95 allows remote attackers to inject arbitrary web script or HTML via the `p_l_back_url_title` parameter.	2023-11-17	6.1	Medium
CVE-2023-44352	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated 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.	2023-11-17	6.1	Medium
CVE-2023-33304	fortinet - multiple products	A use of hard-coded credentials vulnerability in Fortinet FortiClient Windows 7.0.0 - 7.0.9 and 7.2.0 - 7.2.1 allows an attacker to bypass system protections via the use of static credentials.	2023-11-14	5.5	Medium
CVE-2023-36042	microsoft - multiple products	Visual Studio Denial of Service Vulnerability	2023-11-14	5.5	Medium
CVE-2023-36404	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2023-11-14	5.5	Medium
CVE-2023-36406	microsoft - multiple products	Windows Hyper-V Information Disclosure Vulnerability	2023-11-14	5.5	Medium
CVE-2023-36428	microsoft - multiple products	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	2023-11-14	5.5	Medium

CVE-2023-44248	fortinet - multiple products	An improper access control vulnerability [CWE-284] in FortiEDRCollectorWindows version 5.2.0.4549 and below, 5.0.3.1007 and below, 4.0 all may allow a local attacker to prevent the collector service to start in the next system reboot by tampering with some registry keys of the service.	2023-11-14	5.5	Medium
CVE-2022-42879	intel - graphics_driver	NULL pointer dereference in some Intel(R) Arc(TM) & Iris(R) Xe Graphics - WHQL - Windows drivers before version 31.0.101.4255 may allow an authenticated user to potentially enable denial of service via local access.	2023-11-14	5.5	Medium
CVE-2022-43477	intel - unison_software	Incomplete cleanup for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2022-43666	intel - unison_software	Exposure of sensitive system information due to uncleared debug information for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2022-45109	intel - unison_software	Improper initialization for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2022-46299	intel - unison_software	Insufficient control flow management for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2022-46646	intel - unison_software	Exposure of sensitive information to an unauthorized actor for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2022-46647	intel - unison_software	Insertion of sensitive information into log file for some Intel Unison software may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2023-22305	intel - aptio_v_uefi_firmware_integrator_tools	Integer overflow in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated user to potentially enable denial of service via local access.	2023-11-14	5.5	Medium
CVE-2023-25071	intel - iris_xe_graphics	NULL pointer dereference in some Intel(R) Arc(TM) & Iris(R) Xe Graphics - WHQL - Windows Drviers before version 31.0.101.4255 may allow authenticated user to potentially enable denial of service via local access.	2023-11-14	5.5	Medium
CVE-2023-25949	intel - aptio_v_uefi_firmware_integrator_tools	Uncontrolled resource consumption in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated user to potentially enable denial of service via local access.	2023-11-14	5.5	Medium
CVE-2023-26589	intel - aptio_v_uefi_firmware_integrator_tools	Use after free in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allowed an authenticated user to potentially enable denial of service via local access.	2023-11-14	5.5	Medium
CVE-2023-28723	intel - aptio_v_uefi_firmware_integrator_tools	Exposure of sensitive information to an unauthorized actor in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2023-32283	intel - multiple products	Insertion of sensitive information into log file in some Intel(R) On Demand software before versions 1.16.2, 2.1.1, 3.1.0 may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2023-33872	intel - support	Improper access control in the Intel Support android application all verions may allow an authenticated user to potentially enable information disclosure via local access.	2023-11-14	5.5	Medium
CVE-2023-40719	fortinet - multiple products	A use of hard-coded credentials vulnerability in Fortinet FortiAnalyzer and FortiManager 7.0.0 - 7.0.8, 7.2.0 - 7.2.3 and 7.4.0 allows an attacker to access Fortinet private testing data via the use of static credentials.	2023-11-14	5.5	Medium
CVE-2023-36558	microsoft - multiple products	ASP.NET Core - Security Feature Bypass Vulnerability	2023-11-14	5.5	Medium
CVE-2023-39202	zoom - multiple products	Untrusted search path in Zoom Rooms Client for Windows and Zoom VDI Client may allow a privileged user to conduct a denial of service via local access.	2023-11-14	5.5	Medium
CVE-2023-38544	ivanti - multiple products	A logged in user can modify specific files that may lead to unauthorized changes in system-wide configuration settings. This vulnerability could be exploited to compromise the integrity and security of the network on the affected system.	2023-11-15	5.5	Medium
CVE-2023-44296	dell - multiple products	Dell ELab-Navigator, version 3.1.9 contains a hard-coded credential vulnerability. A local attacker could potentially exploit this vulnerability, leading to unauthorized access to sensitive data. Successful exploitation may result in the compromise of confidential user information.	2023-11-16	5.5	Medium
CVE-2023-44340	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium

CVE-2023-44348	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium
CVE-2023-44356	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium
CVE-2023-44357	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium
CVE-2023-44358	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium
CVE-2023-44360	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	2023-11-16	5.5	Medium
CVE-2023-44361	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free 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.	2023-11-16	5.5	Medium
CVE-2023-44327	adobe - multiple products	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44328	adobe - multiple products	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by a Use After Free 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.	2023-11-16	5.5	Medium
CVE-2023-44329	adobe - multiple products	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44331	adobe - photoshop	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44332	adobe - photoshop	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44333	adobe - photoshop	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44334	adobe - multiple products	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium

CVE-2023-44335	adobe - multiple products	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-47044	adobe - multiple products	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-47052	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-47053	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-47054	adobe - multiple products	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-16	5.5	Medium
CVE-2023-44325	adobe - animate	Adobe Animate versions 23.0.2 (and earlier) is 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.	2023-11-17	5.5	Medium
CVE-2023-44326	adobe - dimension	Adobe Dimension versions 3.4.9 (and earlier) is 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.	2023-11-17	5.5	Medium
CVE-2023-47071	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	2023-11-17	5.5	Medium
CVE-2023-36031	microsoft - dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-11-14	5.4	Medium
CVE-2023-36410	microsoft - dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-11-14	5.4	Medium
CVE-2023-36633	fortinet - multiple products	An improper authorization vulnerability [CWE-285] in FortiMail webmail version 7.2.0 through 7.2.2 and before 7.0.5 allows an authenticated attacker to see and modify the title of address book folders of other users via crafted HTTP or HTTPs requests.	2023-11-14	5.4	Medium
CVE-2023-41366	sap - multiple products	Under certain condition SAP NetWeaver Application Server ABAP - versions KERNEL 722, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.94, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT, allows an unauthenticated attacker to access the unintended data due to the lack of restrictions applied which may lead to low impact in confidentiality and no impact on the integrity and availability of the application.	2023-11-14	5.3	Medium
CVE-2023-42480	sap - netweaver_application_server_java	The unauthenticated attacker in NetWeaver AS Java Logon application - version 7.50, can brute force the login functionality to identify the legitimate user ids. This will have an impact on confidentiality but there is no other impact on integrity or availability.	2023-11-14	5.3	Medium
CVE-2023-41570	mikrotik - routeros	MikroTik RouterOS v7.1 to 7.11 was discovered to contain incorrect access control mechanisms in place for the Rest API.	2023-11-14	5.3	Medium
CVE-2023-26364	adobe - css-tools	@adobe/css-tools version 4.3.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a minor denial of service while attempting to parse CSS. Exploitation of this issue does not require user interaction or privileges.	2023-11-17	5.3	Medium
CVE-2023-44339	adobe - multiple products	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	2023-11-16	5	Medium

		such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-5984	schneider-electric - ion8650_firmware	A CWE-494 Download of Code Without Integrity Check vulnerability exists that could allow modified firmware to be uploaded when an authorized admin user begins a firmware update procedure.	2023-11-15	4.9	Medium
CVE-2023-46099	siemens - simatic_pcs_neo	A vulnerability has been identified in SIMATIC PCS neo (All versions < V4.1). There is a stored cross-site scripting vulnerability in the Administration Console of the affected product, that could allow an attacker with high privileges to inject Javascript code into the application that is later executed by another legitimate user.	2023-11-14	4.8	Medium
CVE-2023-5985	schneider-electric - ion8650_firmware	A CWE-79 Improper Neutralization of Input During Web Page Generation vulnerability exists that could cause compromise of a user's browser when an attacker with admin privileges has modified system values.	2023-11-15	4.8	Medium
CVE-2023-22310	intel - aptio_v_uefi_firmware_integrator_tools	Race condition in some Intel(R) Aptio* V UEFI Firmware Integrator Tools may allow an authenticated user to potentially enable denial of service via local access.	2023-11-14	4.7	Medium
CVE-2022-46298	intel - unison_software	Incomplete cleanup for some Intel Unison software may allow a privileged user to potentially enable denial of service via local access.	2023-11-14	4.4	Medium
CVE-2022-46301	intel - unison_software	Improper Initialization for some Intel Unison software may allow a privileged user to potentially enable denial of service via local access.	2023-11-14	4.4	Medium
CVE-2023-39411	intel - unison_software	Improper input validationation for some Intel Unison software may allow a privileged user to potentially enable denial of service via local access.	2023-11-14	4.4	Medium
CVE-2023-40220	intel - nuc6cayh_firmware	Improper buffer restrictions in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	2023-11-14	4.4	Medium
CVE-2023-40540	intel - nuc_11_pro_kit_nuc11tnkv50z_firmware	Non-Transparent Sharing of Microarchitectural Resources in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	2023-11-14	4.4	Medium
CVE-2023-47037	apache - airflow	We failed to apply CVE-2023-40611 in 2.7.1 and this vulnerability was marked as fixed then. Apache Airflow, versions before 2.7.3, 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 2.7.3 or later which has removed the vulnerability.	2023-11-12	4.3	Medium
CVE-2023-38363	ibm - cics_tx	IBM CICS TX Advanced 10.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 260818.	2023-11-13	4.3	Medium
CVE-2023-36026	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-11-16	4.3	Medium
CVE-2023-44355	adobe - multiple products	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to impact a minor integrity feature. Exploitation of this issue does require user interaction.	2023-11-17	4.3	Medium
CVE-2023-36007	microsoft - send_customer_voice_survey_from_dynamics_365	Microsoft Send Customer Voice survey from Dynamics 365 Spoofing Vulnerability	2023-11-14	4.1	Medium
CVE-2023-36016	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-11-14	3.4	Low
CVE-2023-45585	fortinet - multiple products	An insertion of sensitive information into log file vulnerability [CWE-532] in FortiSIEM version 7.0.0, version 6.7.6 and below, version 6.6.3 and below, version 6.5.1 and below, version 6.4.2 and below, version 6.3.3 and below, version 6.2.1 and below, version 6.1.2 and below, version 5.4.0, version 5.3.3 and below may allow an authenticated user to view an encrypted ElasticSearch password via debug log files generated when FortiSIEM is configured with ElasticSearch Event Storage.	2023-11-14	3.3	Low
CVE-2023-47060	adobe - multiple products	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	2023-11-16	3.3	Low

		such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-47072	adobe - multiple products	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-11-17	3.3	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.