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 ١١ أغسطس إلى ١٧ أغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 11th of August to 17th of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-22116	Zabbix	An administrator with restricted permissions can exploit the script execution functionality within the Monitoring Hosts section. The lack of default escaping for script parameters enabled this user ability to execute arbitrary code via the Ping script, thereby compromising infrastructure.	2024-08-12	9.9	Critical
CVE-2024-38063	Microsoft	Windows TCP/IP Remote Code Execution Vulnerability	2024-08-13	9.8	Critical
CVE-2024-38140	Microsoft	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability	2024-08-13	9.8	Critical
CVE-2024-38199	Microsoft	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability	2024-08-13	9.8	Critical
CVE-2024-7593	Ivanti	Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.	2024-08-13	9.8	Critical
CVE-2024-28986	SolarWinds	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. However, out of an abundance of caution, we recommend all Web Help Desk customers apply the patch, which is now available.	2024-08-13	9.8	Critical
CVE-2024-7569	Ivanti	An information disclosure vulnerability in Ivanti ITSM on-prem and Neurons for ITSM versions 2023.4 and earlier allows an unauthenticated attacker to obtain the OIDC client secret via debug information.	2024-08-13	9.6	Critical
CVE-2024-41940	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly validate user input to a privileged command queue. This could allow an authenticated attacker to execute OS commands with elevated privileges.	2024-08-13	9.4	Critical
CVE-2024-38108	Microsoft	Azure Stack Hub Spoofing Vulnerability	2024-08-13	9.3	Critical
CVE-2024-36461	Zabbix	Within Zabbix, users have the ability to directly modify memory pointers in the JavaScript engine.	2024-08-12	9.1	Critical
CVE-2024-38159	Microsoft	Windows Network Virtualization Remote Code Execution Vulnerability	2024-08-13	9.1	Critical
CVE-2024-38160	Microsoft	Windows Network Virtualization Remote Code Execution Vulnerability	2024-08-13	9.1	Critical
CVE-2024-38652	Ivanti	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion.	2024-08-14	9.1	Critical
CVE-2023-26211	Fortinet	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSOAR 7.3.0 through 7.3.2 allows an authenticated, remote attacker to inject arbitrary web script or HTML via the Communications module.	2024-08-13	9	Critical

CVE-2024-39397	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed.	2024-08-14	9	Critical
CVE-2024-39809	F5	The Central Manager user session refresh token does not expire when a user logs out. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-08-14	8.9	High
CVE-2024-36034	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in aggregate reports' search option.	2024-08-12	8.8	High
CVE-2024-36035	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in user session recording.	2024-08-12	8.8	High
CVE-2024-5487	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's export option.	2024-08-12	8.8	High
CVE-2024-5527	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in file auditing configuration.	2024-08-12	8.8	High
CVE-2022-45862	Fortinet	An insufficient session expiration vulnerability [CWE-613] vulnerability in FortiOS 7.2.5 and below, 7.0 all versions, 6.4 all versions; FortiProxy 7.2 all versions, 7.0 all versions; FortiPAM 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions; FortiSwitchManager 7.2.1 and below, 7.0 all versions GUI may allow attackers to re-use websessions after GUI logout, should they manage to acquire the required credentials.	2024-08-13	8.8	High
CVE-2024-38109	Microsoft	An authenticated attacker can exploit an Server-Side Request Forgery (SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network.	2024-08-13	8.8	High
CVE-2024-38114	Microsoft	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38115	Microsoft	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38116	Microsoft	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38120	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38121	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38128	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38130	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38131	Microsoft	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38144	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	8.8	High
CVE-2024-38154	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-38180	Microsoft	Windows SmartScreen Security Feature Bypass Vulnerability	2024-08-13	8.8	High
CVE-2024-38189	Microsoft	Microsoft Project Remote Code Execution Vulnerability	2024-08-13	8.8	High
CVE-2024-41904	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated attacker to conduct brute force attacks against legitimate user credentials or keys.	2024-08-13	8.7	High
CVE-2024-41939	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and elevate their privileges on the application.	2024-08-13	8.7	High
CVE-2024-39778	F5	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	8.7	High
CVE-2024-39792	F5	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	8.7	High
CVE-2024-41727	F5	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.	2024-08-14	8.7	High

		Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.			
CVE-2024-7828	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-15	8.7	High
CVE-2024-7829	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-15	8.7	High
CVE-2024-7830	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-15	8.7	High
CVE-2024-7831	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-15	8.7	High
CVE-2024-7832	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-15	8.7	High
CVE-2024-7849	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This affects the function cgi_create_album of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	2024-08-16	8.7	High

		Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.			
CVE-2024-41976	Siemens	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly validate input in specific VPN configuration fields. This could allow an authenticated remote attacker to execute arbitrary code on the device.	2024-08-13	8.6	High
CVE-2024-36398	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application executes a subset of its services as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.	2024-08-13	8.5	High
CVE-2024-38218	Microsoft	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	2024-08-12	8.4	High
CVE-2024-39401	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	2024-08-14	8.4	High
CVE-2024-39402	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	2024-08-14	8.4	High
CVE-2024-36518	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's dashboard.	2024-08-12	8.3	High
CVE-2024-7570	Ivanti	Improper certificate validation in Ivanti ITSM on-prem and Neurons for ITSM Versions 2023.4 and earlier allows a remote attacker in a MITM position to craft a token that would allow access to ITSM as any user.	2024-08-13	8.3	High
CVE-2024-38211	Microsoft	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-08-13	8.2	High
CVE-2024-41164	F5	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	8.2	High
CVE-2024-36460	Zabbix	The front-end audit log allows viewing of unprotected plaintext passwords, where the passwords are displayed in plain text.	2024-08-12	8.1	High
CVE-2024-29995	Microsoft	Windows Kerberos Elevation of Privilege Vulnerability	2024-08-13	8.1	High
CVE-2024-39400	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link.	2024-08-14	8.1	High

		Confidentiality and integrity impact is high as it affects other admin accounts.			
CVE-2022-27486	Fortinet	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiDDoS version 5.5.0 through 5.5.1, 5.4.2 through 5.4.0, 5.3.0 through 5.3.1, 5.2.0, 5.1.0, 5.0.0, 4.7.0, 4.6.0 and 4.5.0 and FortiDDoS-F version 6.3.0 through 6.3.1, 6.2.0 through 6.2.2, 6.1.0 through 6.1.4 allows an authenticated attacker to execute shell code as `root` via `execute` CLI commands.	2024-08-13	7.8	High
CVE-2024-21757	Fortinet	A unverified password change in Fortinet FortiManager versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, as well as Fortinet FortiAnalyzer versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, allows an attacker to modify admin passwords via the device configuration backup.	2024-08-13	7.8	High
CVE-2024-38084	Microsoft	Microsoft OfficePlus Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38098	Microsoft	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38107	Microsoft	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38117	Microsoft	NTFS Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38125	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38127	Microsoft	Windows Hyper-V Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38133	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38134	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38135	Microsoft	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38141	Microsoft	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38142	Microsoft	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38147	Microsoft	Microsoft DWM Core Library Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38150	Microsoft	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38152	Microsoft	Windows OLE Remote Code Execution Vulnerability	2024-08-13	7.8	High
CVE-2024-38153	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38162	Microsoft	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38169	Microsoft	Microsoft Office Visio Remote Code Execution Vulnerability	2024-08-13	7.8	High
CVE-2024-38171	Microsoft	Microsoft PowerPoint Remote Code Execution Vulnerability	2024-08-13	7.8	High
CVE-2024-38172	Microsoft	Microsoft Excel Remote Code Execution Vulnerability	2024-08-13	7.8	High
CVE-2024-38177	Microsoft	Windows App Installer Spoofing Vulnerability	2024-08-13	7.8	High
CVE-2024-38184	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38185	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38186	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38187	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38191	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38193	Microsoft	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38195	Microsoft	Azure CycleCloud Remote Code Execution Vulnerability	2024-08-13	7.8	High
CVE-2024-38196	Microsoft	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38215	Microsoft	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	High
CVE-2024-38163	Microsoft	Windows Update Stack Elevation of Privilege Vulnerability	2024-08-14	7.8	High
CVE-2024-41858	Adobe	InCopy versions 18.5.2, 19.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-41864	Adobe	Substance3D - Designer versions 13.1.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-20789	Adobe	Dimension versions 3.4.11 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.	2024-08-14	7.8	High
CVE-2024-34117	Adobe	Photoshop Desktop versions 24.7.3, 25.9.1 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.	2024-08-14	7.8	High
CVE-2024-34124	Adobe	Dimension versions 3.4.11 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	2024-08-14	7.8	High

		issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-34133	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39383	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	High
CVE-2024-39386	Adobe	Bridge versions 13.0.8, 14.1.1 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.	2024-08-14	7.8	High
CVE-2024-39388	Adobe	Substance3D - Stager versions 3.0.2 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.	2024-08-14	7.8	High
CVE-2024-39389	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	High
CVE-2024-39390	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39391	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39393	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39394	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39422	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	High
CVE-2024-39423	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-39424	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	High
CVE-2024-39426	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-41830	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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	2024-08-14	7.8	High

		issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-41831	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	High
CVE-2024-41840	Adobe	Bridge versions 13.0.8, 14.1.1 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.	2024-08-14	7.8	High
CVE-2024-41850	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	High
CVE-2024-41851	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-41852	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	High
CVE-2024-41853	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	High
CVE-2024-41856	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	High
CVE-2024-41865	Adobe	Dimension versions 3.4.11 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious file into the search path, which the application might execute instead of the legitimate file. This could occur if the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction.	2024-08-14	7.8	High
CVE-2024-31333	Google	In _MMU_AllocLevel of mmu_common.c, there is a possible arbitrary code execution due to an integer overflow. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.8	High
CVE-2024-34741	Google	In setForceHideNonSystemOverlayWindowIfNeeded of WindowState.java, there is a possible way for message content to be visible on the screensaver while lock screen visibility settings are restricted by the user 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.	2024-08-15	7.8	High
CVE-2024-34743	Google	In setTransactionState of SurfaceFlinger.cpp, there is a possible way to perform tapjacking 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.	2024-08-15	7.8	High
CVE-2024-2175	Lenovo	An insecure permissions vulnerability was reported in Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a local attacker to escalate privileges.	2024-08-16	7.8	High
CVE-2024-4763	Lenovo	An insecure driver vulnerability was reported in Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a local attacker to escalate privileges to kernel.	2024-08-16	7.8	High
CVE-2024-42271	Linux	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking	2024-08-17	7.8	High

		care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv.			
CVE-2024-42284	Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address.	2024-08-17	7.8	High

CVE-2024-42285	Linux	In the Linux kernel, the following vulnerability has been resolved:
		
		RDMA/iwcm: Fix a use-after-free related to destroying CM IDs
		
		iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with
		an existing struct iw_cm_id (cm_id) as follows:
		
		conn_id->cm_id.iw = cm_id;
		cm_id->context = conn_id;
		cm_id->cm_handler = cma_iw_handler;
		
		rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make
		sure that cm_work_handler() does not trigger a use-after-free by only
		freeing of the struct rdma_id_private after all pending work has finished.
			2024-08-17	7.8	High

CVE-2024-42301	Linux	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport]	2024-08-17	7.8	High
CVE-2024-42302	Linux	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops. That's because pci_bridge_wait_for_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit 53b54ad074de ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0	2024-08-17	7.8	High

		RIP: pci_bus_read_config_dword+0x17/0x50 pci_dev_wait() pci_bridge_wait_for_secondary_bus() dpc_reset_link() pcie_do_recovery() dpc_handler()			
CVE-2024-42313	Linux	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close.	2024-08-17	7.8	High
CVE-2024-42314	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix extent map use-after-free when adding pages to compressed bio At add_ra_bio_pages() we are accessing the extent map to calculate 'add_size' after we dropped our reference on the extent map, resulting in a use-after-free. Fix this by computing 'add_size' before dropping our extent map reference.	2024-08-17	7.8	High
CVE-2024-43852	Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ltc2991) re-order conditions to fix off by one bug LTC2991_T_INT_CH_NR is 4. The st->temp_en[] array has LTC2991_MAX_CHANNEL (4) elements. Thus if "channel" is equal to LTC2991_T_INT_CH_NR then we have read one element beyond the end of the array. Flip the conditions around so that we check if "channel" is valid before using it as an array index.	2024-08-17	7.8	High
CVE-2024-43858	Linux	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree	2024-08-17	7.8	High
CVE-2024-39399	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed.	2024-08-14	7.7	High
CVE-2024-39406	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed.	2024-08-14	7.7	High
CVE-2024-34731	Google	In multiple functions of TranscodingResourcePolicy.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.7	High
CVE-2024-34734	Google	In onForegroundServiceButtonClicked of FooterActionsViewModel.kt, there is a possible way to disable the active VPN app from the lockscreen due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.7	High
CVE-2024-34737	Google	In ensureSetPipAspectRatioQuotaTracker of ActivityClientController.java, there is a possible way to generate unmovable and undeletable pip windows 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.	2024-08-15	7.7	High
CVE-2024-34738	Google	In multiple functions of AppOpsService.java, there is a possible way for unprivileged apps to read their own restrictRead app-op states due to a logic error in the code. This could lead to local	2024-08-15	7.7	High

		escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2024-34739	Google	In shouldRestrictOverlayActivities of UsbProfileGroupSettingsManager.java, there is a possible escape from SUW due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-08-15	7.7	High
CVE-2024-34740	Google	In attributeBytesBase64 and attributeBytesHex of BinaryXmlSerializer.java, there is a possible arbitrary XML injection due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.7	High
CVE-2024-41905	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not have access control for accessing the files. This could allow an authenticated attacker with low privilege's to get access to sensitive information.	2024-08-13	7.6	High
CVE-2024-39403	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information.	2024-08-14	7.6	High
CVE-2024-36462	Zabbix	Uncontrolled resource consumption refers to a software vulnerability where a attacker or system uses excessive resources, such as CPU, memory, or network bandwidth, without proper limitations or controls. This can cause a denial-of-service (DoS) attack or degrade the performance of the affected system.	2024-08-12	7.5	High
CVE-2024-41903	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application mounts the container's root filesystem with read and write privileges. This could allow an attacker to alter the container's filesystem leading to unauthorized modifications and data corruption.	2024-08-13	7.5	High
CVE-2024-40697	IBM	IBM Common Licensing 9.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 297895.	2024-08-13	7.5	High
CVE-2024-35124	IBM	A vulnerability in the combination of the OpenBMC's FW1050.00 through FW1050.10, FW1030.00 through FW1030.50, and FW1020.00 through FW1020.60 default password and session management allow an attacker to gain administrative access to the BMC. IBM X-Force ID: 290674.	2024-08-13	7.5	High
CVE-2024-37968	Microsoft	Windows DNS Spoofing Vulnerability	2024-08-13	7.5	High
CVE-2024-38126	Microsoft	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38132	Microsoft	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38138	Microsoft	Windows Deployment Services Remote Code Execution Vulnerability	2024-08-13	7.5	High
CVE-2024-38145	Microsoft	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38146	Microsoft	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38148	Microsoft	Windows Secure Channel Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38168	Microsoft	.NET and Visual Studio Denial of Service Vulnerability	2024-08-13	7.5	High
CVE-2024-38178	Microsoft	Scripting Engine Memory Corruption Vulnerability	2024-08-13	7.5	High
CVE-2024-38198	Microsoft	Windows Print Spooler Elevation of Privilege Vulnerability	2024-08-13	7.5	High
CVE-2024-36136	Ivanti	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.	2024-08-14	7.5	High
CVE-2024-37399	Ivanti	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.	2024-08-14	7.5	High
CVE-2024-38653	Ivanti	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server.	2024-08-14	7.5	High
CVE-2023-50314	IBM	IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.8 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 274713.	2024-08-14	7.5	High
CVE-2024-39398	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized	2024-08-14	7.4	High

		access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high.			
CVE-2023-7066	Siemens	The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	2024-08-12	7.3	High
CVE-2024-41908	Siemens	A vulnerability has been identified in NX (All versions < V2406.3000). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2024-08-13	7.3	High
CVE-2024-41977	Siemens	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly enforce isolation between user sessions in their web server component. This could allow an authenticated remote attacker to escalate their privileges on the devices.	2024-08-13	7.3	High
CVE-2022-33162	IBM	IBM Security Directory Integrator 7.2.0 and Security Verify Directory Integrator 10.0.0 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. IBM X-Force ID: 228570.	2024-08-16	7.3	High
CVE-2024-37373	Ivanti	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE.	2024-08-14	7.2	High
CVE-2024-41978	Siemens	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected	2024-08-13	7.1	High

		devices insert sensitive information about the generation of 2FA tokens into log files. This could allow an authenticated remote attacker to forge 2FA tokens of other users.			
CVE-2024-38170	Microsoft	Microsoft Excel Remote Code Execution Vulnerability	2024-08-13	7.1	High
CVE-2024-34127	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.1	High
CVE-2024-38106	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7	High
CVE-2024-38136	Microsoft	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	2024-08-13	7	High
CVE-2024-38137	Microsoft	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	2024-08-13	7	High
CVE-2024-38157	Microsoft	Azure IoT SDK Remote Code Execution Vulnerability	2024-08-13	7	High
CVE-2024-38158	Microsoft	Azure IoT SDK Remote Code Execution Vulnerability	2024-08-13	7	High
CVE-2024-38201	Microsoft	Azure Stack Hub Elevation of Privilege Vulnerability	2024-08-13	7	High
CVE-2024-39420	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7	High
CVE-2024-39425	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high.	2024-08-14	7	High
CVE-2024-41682	Siemens	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated remote attacker to conduct brute force attacks against legitimate user passwords.	2024-08-13	6.9	Medium
CVE-2024-41683	Siemens	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce a strong user password policy. This could facilitate a brute force attack against legitimate user passwords.	2024-08-13	6.9	Medium
CVE-2024-6768	Microsoft	A Denial of Service in CLFS.sys in Microsoft Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 allows a malicious authenticated low-privilege user to cause a Blue Screen of Death via a forced call to the KeBugCheckEx function.	2024-08-12	6.8	Medium
CVE-2024-38161	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-08-13	6.8	Medium
CVE-2024-38223	Microsoft	Windows Initial Machine Configuration Elevation of Privilege Vulnerability	2024-08-13	6.8	Medium
CVE-2024-38173	Microsoft	Microsoft Outlook Remote Code Execution Vulnerability	2024-08-13	6.7	Medium
CVE-2024-38200	Microsoft	Microsoft Office Spoofing Vulnerability	2024-08-12	6.5	Medium
CVE-2024-38219	Microsoft	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-08-12	6.5	Medium
CVE-2024-38165	Microsoft	Windows Compressed Folder Tampering Vulnerability	2024-08-13	6.5	Medium
CVE-2024-38167	Microsoft	.NET and Visual Studio Information Disclosure Vulnerability	2024-08-13	6.5	Medium
CVE-2024-38197	Microsoft	Microsoft Teams for iOS Spoofing Vulnerability	2024-08-13	6.5	Medium
CVE-2024-38213	Microsoft	Windows Mark of the Web Security Feature Bypass Vulnerability	2024-08-13	6.5	Medium
CVE-2024-38214	Microsoft	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	2024-08-13	6.5	Medium
CVE-2024-31882	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287614.	2024-08-14	6.5	Medium
CVE-2024-35136	IBM	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) federated server 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 291307.	2024-08-14	6.5	Medium
CVE-2024-35152	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation. IBM X-Force ID: 292639.	2024-08-14	6.5	Medium
CVE-2024-37529	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation. IBM X-Force ID: 294295.	2024-08-14	6.5	Medium

CVE-2024-40705	IBM	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279.	2024-08-15	6.5	Medium
CVE-2024-4781	Lenovo	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to crash printer communications until the system is rebooted.	2024-08-16	6.5	Medium
CVE-2024-4782	Lenovo	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to disrupt the printer's functionality until a manual system reboot occurs.	2024-08-16	6.5	Medium
CVE-2024-5209	Lenovo	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printing capabilities until the system is rebooted.	2024-08-16	6.5	Medium
CVE-2024-5210	Lenovo	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to prevent printer services from being reachable until the system is rebooted.	2024-08-16	6.5	Medium
CVE-2024-6004	Lenovo	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printer connections until the system is rebooted.	2024-08-16	6.5	Medium
CVE-2023-38018	IBM	IBM Aspera Shares 1.10.0 PL2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 260574.	2024-08-12	6.3	Medium
CVE-2024-41906	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application does not properly handle cacheable HTTP responses in the web service. This could allow an attacker to read and modify data stored in the local cache.	2024-08-13	6.3	Medium
CVE-2024-39408	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	2024-08-14	6.3	Medium
CVE-2024-39409	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	2024-08-14	6.3	Medium
CVE-2024-37028	F5	BIG-IP Next Central Manager may allow an attacker to lock out an account that has never been logged in. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	6.3	Medium
CVE-2024-25024	IBM	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 281430.	2024-08-15	6.2	Medium
CVE-2024-22121	Zabbix	A non-admin user can change or remove important features within the Zabbix Agent application, thus impacting the integrity and availability of the application.	2024-08-12	6.1	Medium
CVE-2024-41681	Siemens	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). The web server of affected products is configured to support weak ciphers by default. This could allow an unauthenticated attacker in an on-path position to to read and modify any data passed over the connection between legitimate clients and the affected device.	2024-08-13	6	Medium
CVE-2024-27267	IBM	The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 7.1.5.18 and 8.0.0.0 through 8.0.8.26 is vulnerable to remote denial of service, caused by a race condition in the management of ORB listener threads. IBM X-Force ID: 284573.	2024-08-14	5.9	Medium
CVE-2024-31905	IBM	IBM QRadar Network Packet Capture 7.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 289858.	2024-08-15	5.9	Medium
CVE-2024-38483	Dell	Dell BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-08-14	5.8	Medium
CVE-2024-43472	Microsoft	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-08-16	5.8	Medium
CVE-2024-7347	F5	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-	2024-08-14	5.7	Medium

		read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.			
CVE-2024-28799	IBM	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 displays sensitive data improperly during back-end commands which may result in the unexpected disclosure of this information. IBM X-Force ID: 287173.	2024-08-14	5.6	Medium
CVE-2024-42258	Linux	In the Linux kernel, the following vulnerability has been resolved: mm: huge_memory: use !CONFIG_64BIT to relax huge page alignment on 32 bit machines Yves-Alexis Perez reported commit 4ef9ad19e176 ("mm: huge_memory: don't force huge page alignment on 32 bit") didn't work for x86_32 [1]. It is because x86_32 uses CONFIG_X86_32 instead of CONFIG_32BIT. !CONFIG_64BIT should cover all 32 bit machines. [1] https://lore.kernel.org/linux-mm/CAHbLzkr1LwH3pcTgM+aGQ31ip2bKqiqEQ8=FQB+t2c3dhNKNHA@mail.gmail.com/	2024-08-12	5.5	Medium
CVE-2024-36505	Fortinet	An improper access control vulnerability [CWE-284] in FortiOS 7.4.0 through 7.4.3, 7.2.5 through 7.2.7, 7.0.12 through 7.0.14 and 6.4.x may allow an attacker who has already successfully obtained write access to the underlying system (via another hypothetical exploit) to bypass the file integrity checking system.	2024-08-13	5.5	Medium
CVE-2024-38118	Microsoft	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	2024-08-13	5.5	Medium
CVE-2024-38122	Microsoft	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	2024-08-13	5.5	Medium
CVE-2024-38151	Microsoft	Windows Kernel Information Disclosure Vulnerability	2024-08-13	5.5	Medium
CVE-2024-38155	Microsoft	Security Center Broker Information Disclosure Vulnerability	2024-08-13	5.5	Medium
CVE-2024-41860	Adobe	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	Medium
CVE-2024-41861	Adobe	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	Medium
CVE-2024-41862	Adobe	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	Medium
CVE-2024-41863	Adobe	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	Medium
CVE-2024-39410	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	2024-08-14	5.5	Medium
CVE-2024-20790	Adobe	Dimension versions 3.4.11 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.	2024-08-14	5.5	Medium
CVE-2024-34118	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-34125	Adobe	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive	2024-08-14	5.5	Medium

		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.			
CVE-2024-34126	Adobe	Dimension versions 3.4.11 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.	2024-08-14	5.5	Medium
CVE-2024-34134	Adobe	Illustrator versions 28.5, 27.9.4 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.	2024-08-14	5.5	Medium
CVE-2024-34135	Adobe	Illustrator versions 28.5, 27.9.4 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.	2024-08-14	5.5	Medium
CVE-2024-34136	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-34137	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-34138	Adobe	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-39387	Adobe	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-39395	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-41832	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	Medium
CVE-2024-41833	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	Medium
CVE-2024-41834	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	Medium
CVE-2024-41835	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	Medium
CVE-2024-41854	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	Medium
CVE-2024-41866	Adobe	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an	2024-08-14	5.5	Medium

		application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-52889	Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address: 000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50 sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40	2024-08-17	5.5	Medium

		RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc			
CVE-2024-42262	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the performance extension If fetching of userspace memory fails during the main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 484de39fa5f5b7bd0c5f2e2c5265167250ef7501)	2024-08-17	5.5	Medium
CVE-2024-42263	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the timestamp extension If fetching of userspace memory fails during the main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 753ce4fea62182c77e1691ab4f9022008f25b62e)	2024-08-17	5.5	Medium
CVE-2024-42268	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates devlink on reload actions performed on that host, it misses taking devlink lock before calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: WARNING: CPU: 4 PID: 1164 at net/devlink/core.c:261 devl_assert_locked+0x3e/0x50 … CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS-2028TP-DECTR/X10DRT-PT, BIOS 2.0 12/18/2015 Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 … Call Trace: <TASK> ? __warn+0xa4/0x210	2024-08-17	5.5	Medium

		? devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_locked+0x3e/0x50 devlink_notify+0x88/0x2b0 ? mlx5_attach_device+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+0x4b6/0xbb0 […]			
CVE-2024-42269	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init(). ip6table_nat_table_init() accesses net->gen->ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys(). Let's call register_pernet_subsys() before xt_register_template().	2024-08-17	5.5	Medium
CVE-2024-42270	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in iptable_nat_table_init(). We had a report that iptables-restore sometimes triggered null-ptr-deref at boot time. [0] The problem is that iptable_nat_table_init() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call iptable_nat_table_init() that accesses net_generic(net, iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_template(). [0]: bpfilter: Loaded bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013 PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1 Hardware name: Amazon EC2 c6i.4xlarge/, BIOS 1.0 10/16/2017 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 c0 75 38 41 83 c7 01 49 83 c6 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843cd0 EFLAGS: 00010246 RAX: 0000000000000013 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08: ffff9f4b07f77258 R09: ffff9f4b07f77240 R10: 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15: 0000000000000004 FS: 00007f6284340000(0000) GS:ffff9f51fe280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000	2024-08-17	5.5	Medium

		DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h:75 arch/x86/mm/fault.c:1470 arch/x86/mm/fault.c:1518) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat xt_find_table_lock (net/netfilter/x_tables.c:1259) xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965) ? security_capable (security/security.c:809 (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bpfilter_kern.c:52) bpfilter nf_getsockopt (net/netfilter/nf_sockopt.c:116) ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2342 net/socket.c:2339 net/socket.c:2339) do_syscall_64 (arch/x86/entry/common.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) RIP: 0033:0x7f62844685ee Code: 48 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 09 RSP: 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX: 0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000004 RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11: 0000000000000246 R12: 00007ffd1f83e3b2 R13: 00007f6284 ---truncated---			
CVE-2024-42282	Linux	In the Linux kernel, the following vulnerability has been resolved: net: mediatek: Fix potential NULL pointer dereference in dummy net_device handling Move the freeing of the dummy net_device from mtk_free_dev() to mtk_remove(). Previously, if alloc_netdev_dummy() failed in mtk_probe(), eth->dummy_dev would be NULL. The error path would then call mtk_free_dev(), which in turn called free_netdev() assuming dummy_dev was allocated (but it was not), potentially causing a NULL pointer dereference. By moving free_netdev() to mtk_remove(), we ensure it's only called when mtk_probe() has succeeded and dummy_dev is fully allocated. This addresses a potential NULL pointer dereference detected by Smatch[1].	2024-08-17	5.5	Medium
CVE-2024-42283	Linux	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity):	2024-08-17	5.5	Medium

		# ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure.			
CVE-2024-42294	Linux	In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between sd_remove & sd_release Our test report the following hung task: [2538.459400] INFO: task "kworker/0:0":7 blocked for more than 188 seconds. [2538.459427] Call trace: [2538.459430] __switch_to+0x174/0x338 [2538.459436] __schedule+0x628/0x9c4 [2538.459442] schedule+0x7c/0xe8 [2538.459447] schedule_preempt_disabled+0x24/0x40 [2538.459453] __mutex_lock+0x3ec/0xf04 [2538.459456] __mutex_lock_slowpath+0x14/0x24 [2538.459459] mutex_lock+0x30/0xd8 [2538.459462] del_gendisk+0xdc/0x350 [2538.459466] sd_remove+0x30/0x60 [2538.459470] device_release_driver_internal+0x1c4/0x2c4 [2538.459474] device_release_driver+0x18/0x28 [2538.459478] bus_remove_device+0x15c/0x174 [2538.459483] device_del+0x1d0/0x358 [2538.459488] __scsi_remove_device+0xa8/0x198 [2538.459493] scsi_forget_host+0x50/0x70 [2538.459497] scsi_remove_host+0x80/0x180 [2538.459502] usb_stor_disconnect+0x68/0xf4 [2538.459506] usb_unbind_interface+0xd4/0x280 [2538.459510] device_release_driver_internal+0x1c4/0x2c4 [2538.459514] device_release_driver+0x18/0x28 [2538.459518] bus_remove_device+0x15c/0x174 [2538.459523] device_del+0x1d0/0x358 [2538.459528] usb_disable_device+0x84/0x194 [2538.459532] usb_disconnect+0xec/0x300 [2538.459537] hub_event+0xb80/0x1870 [2538.459541] process_scheduled_works+0x248/0x4dc [2538.459545] worker_thread+0x244/0x334 [2538.459549] kthread+0x114/0x1bc [2538.461001] INFO: task "fsck.":15415 blocked for more than 188 seconds. [2538.461014] Call trace: [2538.461016] __switch_to+0x174/0x338 [2538.461021] __schedule+0x628/0x9c4 [2538.461025] schedule+0x7c/0xe8 [2538.461030] blk_queue_enter+0xc4/0x160 [2538.461034] blk_mq_alloc_request+0x120/0x1d4 [2538.461037] scsi_execute_cmd+0x7c/0x23c [2538.461040] ioctl_internal_command+0x5c/0x164 [2538.461046] scsi_set_medium_removal+0x5c/0xb0 [2538.461051] sd_release+0x50/0x94 [2538.461054] blkdev_put+0x190/0x28c [2538.461058] blkdev_release+0x28/0x40 [2538.461063] __fput+0xf8/0x2a8 [2538.461066] __fput_sync+0x28/0x5c [2538.461070] __arm64_sys_close+0x84/0xe8 [2538.461073] invoke_syscall+0x58/0x114 [2538.461078] el0_svc_common+0xac/0xe0 [2538.461082] do_el0_svc+0x1c/0x28 [2538.461087] el0_svc+0x38/0x68 [2538.461090] el0t_64_sync_handler+0x68/0xbc [2538.461093] el0t_64_sync+0x1a8/0x1ac T1: T2: sd_remove del_gendisk __blk_mark_disk_dead blk_freeze_queue_start ++q->mq_freeze_depth	2024-08-17	5.5	Medium

		bdev_release mutex_lock(&disk->open_mutex) sd_release scsi_execute_cmd blk_queue_enter wait_event(!q->mq_freeze_depth) mutex_lock(&disk->open_mutex) SCSI does not set GD_OWNS_QUEUE, so QUEUE_FLAG_DYING is not set in this scenario. This is a classic ABBA deadlock. To fix the deadlock, make sure we don't try to acquire disk->open_mutex after freezing the queue.			
CVE-2024-42309	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	2024-08-17	5.5	Medium
CVE-2024-42310	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	2024-08-17	5.5	Medium
CVE-2024-42315	Linux	In the Linux kernel, the following vulnerability has been resolved: exfat: fix potential deadlock on __exfat_get_dentry_set When accessing a file with more entries than ES_MAX_ENTRY_NUM, the bh-array is allocated in __exfat_get_entry_set. The problem is that the bh-array is allocated with GFP_KERNEL. It does not make sense. In the following cases, a deadlock for sbi->s_lock between the two processes may occur. CPU0 CPU1 ---- ---- kswapd balance_pgdat lock(fs_reclaim) exfat_iterate lock(&sbi->s_lock) exfat_readdir exfat_get_uniname_from_ext_entry exfat_get_dentry_set __exfat_get_dentry_set kmalloc_array ... lock(fs_reclaim) ... evict exfat_evict_inode lock(&sbi->s_lock) To fix this, let's allocate bh-array with GFP_NOFS.	2024-08-17	5.5	Medium
CVE-2024-42316	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/mglru: fix div-by-zero in vmpressure_calc_level() evict_folios() uses a second pass to reclaim folios that have gone through page writeback and become clean before it finishes the first pass, since folio_rotate_reclaimable() cannot handle those folios due to the isolation. The second pass tries to avoid potential double counting by deducting scan_control->nr_scanned. However, this can result in underflow of	2024-08-17	5.5	Medium

		nr_scanned, under a condition where shrink_folio_list() does not increment nr_scanned, i.e., when folio_trylock() fails. The underflow can cause the divisor, i.e., scale=scanned+reclaimed in vmpressure_calc_level(), to become zero, resulting in the following crash: [exception RIP: vmpressure_work_fn+101] process_one_work at ffffffffa3313f2b Since scan_control->nr_scanned has no established semantics, the potential double counting has minimal risks. Therefore, fix the problem by not deducting scan_control->nr_scanned in evict_folios().			
CVE-2024-43828	Linux	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit When doing fast_commit replay an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem!	2024-08-17	5.5	Medium
CVE-2024-43833	Linux	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix NULL pointer dereference in adding ancillary links In v4l2_async_create_ancillary_links(), ancillary links are created for lens and flash sub-devices. These are sub-device to sub-device links and if the async notifier is related to a V4L2 device, the source sub-device of the ancillary link is NULL, leading to a NULL pointer dereference. Check the notifier's sd field is non-NULL in v4l2_async_create_ancillary_links(). [Sakari Ailus: Reword the subject and commit messages slightly.]	2024-08-17	5.5	Medium
CVE-2024-43836	Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethtool: pse-pd: Fix possible null-deref Fix a possible null dereference when a PSE supports both c33 and PoDL, but only one of the netlink attributes is specified. The c33 or PoDL PSE capabilities are already validated in the ethnl_set_pse_validate() call.	2024-08-17	5.5	Medium
CVE-2024-43837	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix null pointer dereference in resolve_prog_type() for BPF_PROG_TYPE_EXT When loading a EXT program without specifying `attr->attach_prog_fd`, the `prog->aux->dst_prog` will be null. At this time, calling resolve_prog_type() anywhere will result in a null pointer dereference. Example stack trace: [8.107863] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000004 [8.108262] Mem abort info:	2024-08-17	5.5	Medium

		[8.108384] ESR = 0x0000000096000004 [8.108547] EC = 0x25: DABT (current EL), IL = 32 bits [8.108722] SET = 0, FnV = 0 [8.108827] EA = 0, S1PTW = 0 [8.108939] FSC = 0x04: level 0 translation fault [8.109102] Data abort info: [8.109203] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [8.109399] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [8.109614] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [8.109836] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101354000 [8.110011] [0000000000000004] pgd=0000000000000000, p4d=0000000000000000 [8.112624] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [8.112783] Modules linked in: [8.113120] CPU: 0 PID: 99 Comm: may_access_dire Not tainted 6.10.0-rc3-next-20240613-dirty #1 [8.113230] Hardware name: linux,dummy-virt (DT) [8.113390] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [8.113429] pc : may_access_direct_pkt_data+0x24/0xa0 [8.113746] lr : add_subprog_and_kfunc+0x634/0x8e8 [8.113798] sp : ffff80008283b9f0 [8.113813] x29: ffff80008283b9f0 x28: ffff800082795048 x27: 0000000000000001 [8.113881] x26: ffff0000c0bb2600 x25: 0000000000000000 x24: 0000000000000000 [8.113897] x23: ffff0000c1134000 x22: 000000000001864f x21: ffff0000c1138000 [8.113912] x20: 0000000000000001 x19: ffff0000c12b8000 x18: ffffffffffffffff [8.113929] x17: 0000000000000000 x16: 0000000000000000 x15: 0720072007200720 [8.113944] x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 [8.113958] x11: 0720072007200720 x10: 0000000000f9fca4 x9 : ffff80008021f4e4 [8.113991] x8 : 0101010101010101 x7 : 746f72705f6d656d x6 : 000000001e0e0f5f [8.114006] x5 : 000000000001864f x4 : ffff0000c12b8000 x3 : 000000000000001c [8.114020] x2 : 0000000000000002 x1 : 0000000000000000 x0 : 0000000000000000 [8.114126] Call trace: [8.114159] may_access_direct_pkt_data+0x24/0xa0 [8.114202] bpf_check+0x3bc/0x28c0 [8.114214] bpf_prog_load+0x658/0xa58 [8.114227] __sys_bpf+0xc50/0x2250 [8.114240] __arm64_sys_bpf+0x28/0x40 [8.114254] invoke_syscall.constprop.0+0x54/0xf0 [8.114273] do_el0_svc+0x4c/0xd8 [8.114289] el0_svc+0x3c/0x140 [8.114305] el0t_64_sync_handler+0x134/0x150 [8.114331] el0t_64_sync+0x168/0x170 [8.114477] Code: 7100707f 54000081 f9401c00 f9403800 (b9400403) [8.118672] ---[end trace 0000000000000000]--- One way to fix it is by forcing `attach_prog_fd` non-empty when bpf_prog_load(). But this will lead to `libbpf_probe_bpf_prog_type` API broken which use verifier log to probe prog type and will log nothing if we reject invalid EXT prog before bpf_check(). Another way is by adding null check in resolve_prog_type(). The issue was introduced by commit 4a9c7bbe2ed4 ("bpf: Resolve to prog->aux->dst_prog->type only for BPF_PROG_TYPE_EXT") which wanted to correct type resolution for BPF_PROG_TYPE_TRACING programs. Before that, the type resolution of BPF_PROG_TYPE_EXT prog actually follows the logic below: prog->aux->dst_prog ? prog->aux->dst_prog->type : prog->type; It implies that when EXT program is not yet attached to `dst_prog`,			

		the prog type should be EXT itself. This code worked fine in the past. So just keep using it. Fix this by returning `prog->type` for BPF_PROG_TYPE_EXT if `dst_prog` is not present in resolve_prog_type().			

CVE-2024-43853	Linux	In the Linux kernel, the following vulnerability has been resolved:
		
		cgroup/cpuset: Prevent UAF in proc_cpuset_show()
		
		An UAF can happen when /proc/cpuset is read as reported in [1].
		
		This can be reproduced by the following methods:
		1.add an mdelay(1000) before acquiring the cgroup_lock In the cgroup_path_ns function.
		2.$cat /proc/<pid>/cpuset repeatly.
		3.$mount -t cgroup -o cpuset cpuset /sys/fs/cgroup/cpuset/
		$umount /sys/fs/cgroup/cpuset/ repeatly.
		
		The race that cause this bug can be shown as below:
		
		(umount) | (cat /proc/<pid>/cpuset)
		css_release | proc_cpuset_show
		css_release_work_fn | css = task_get_css(tsk, cpuset_cgrp_id);
		css_free_rwork_fn | cgroup_path_ns(css->cgroup, ...);
		cgroup_destroy_root | mutex_lock(&cgroup_mutex);
		rebind_subsystems |
		cgroup_free_root |
		| // cgrp was freed, UAF
		| cgroup_path_ns_locked(cgrp,..);
		
		When the cpuset is initialized, the root node top_cpuset.css.cgrp will point to &cgrp_dfl_root.cgrp. In cgroup v1, the mount operation will
		allocate cgroup_root, and top_cpuset.css.cgrp will point to the allocated
		&cgroup_root.cgrp. When the umount operation is executed, top_cpuset.css.cgrp will be rebound to &cgrp_dfl_root.cgrp.
		
		The problem is that when rebinding to cgrp_dfl_root, there are cases
		where the cgroup_root allocated by setting up the root for cgroup v1
		is cached. This could lead to a Use-After-Free (UAF) if it is subsequently freed. The descendant cgroups of cgroup v1 can only be
		freed after the css is released. However, the css of the root will never
		be released, yet the cgroup_root should be freed when it is unmounted.
		This means that obtaining a reference to the css of the root does not guarantee that css.cgrp->root will not be freed.
		
		Fix this problem by using rcu_read_lock in proc_cpuset_show().
		As cgroup_root is kfree_rcu after commit d23b5c577715
		("cgroup: Make operations on the cgroup root_list RCU safe"),
		css->cgroup won't be freed during the critical section.
		To call cgroup_path_ns_locked, css_set_lock is needed, so it is safe to
		replace task_get_css with task_css.
		
		[1]
		https://syzkaller.appspot.com/bug?extid=9b1ff7be974a403aa4cd
			2024-08-17	5.5	Medium

CVE-2024-43854	Linux	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media Metadata added by bio_integrity_prep is using plain kmalloc, which leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadata the entire buffer leaks kernel memory. Fix this by adding the __GFP_ZERO flag to allocations for writes.	2024-08-17	5.5	Medium
CVE-2024-43855	Linux	In the Linux kernel, the following vulnerability has been resolved: md: fix deadlock between mddev_suspend and flush bio	2024-08-17	5.5	Medium

		Deadlock occurs when mddev is being suspended while some flush bio is in progress. It is a complex issue. T1. the first flush is at the ending stage, it clears 'mddev->flush_bio' and tries to submit data, but is blocked because mddev is suspended by T4. T2. the second flush sets 'mddev->flush_bio', and attempts to queue md_submit_flush_data(), which is already running (T1) and won't execute again if on the same CPU as T1. T3. the third flush inc active_io and tries to flush, but is blocked because 'mddev->flush_bio' is not NULL (set by T2). T4. mddev_suspend() is called and waits for active_io dec to 0 which is inc by T3. T1 T2 T3 T4 (flush 1) (flush 2) (third 3) (suspend) md_submit_flush_data mddev->flush_bio = NULL; . . md_flush_request . mddev->flush_bio = bio . queue submit_flushes . . . . md_handle_request . . active_io + 1 . . md_flush_request . . wait !mddev->flush_bio . . . . mddev_suspend . . wait !active_io . . . submit_flushes . queue_work md_submit_flush_data . //md_submit_flush_data is already running (T1) . md_handle_request wait resume The root issue is non-atomic inc/dec of active_io during flush process. active_io is dec before md_submit_flush_data is queued, and inc soon after md_submit_flush_data() run. md_flush_request active_io + 1 submit_flushes active_io - 1 md_submit_flush_data md_handle_request active_io + 1 make_request active_io - 1 If active_io is dec after md_handle_request() instead of within submit_flushes(), make_request() can be called directly intead of md_handle_request() in md_submit_flush_data(), and active_io will only inc and dec once in the whole flush process. Deadlock will be fixed. Additionally, the only difference between fixing the issue and before is that there is no return error handling of make_request(). But after previous patch cleaned md_write_start(), make_requst() only return error in raid5_make_request() by dm-raid, see commit 41425f96d7aa ("dm-raid456, md/raid456: fix a deadlock for dm-raid456 while io concurrent with reshape)". Since dm always splits data and flush operation into two separate io, io size of flush submitted by dm always is 0,			

		make_request() will not be called in md_submit_flush_data(). To prevent future modifications from introducing issues, add WARN_ON to ensure make_request() no error is returned in this context.			
CVE-2024-43856	Linux	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03	2024-08-17	5.5	Medium
CVE-2024-43857	Linux	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix null reference error when checking end of zone This patch fixes a potentially null pointer being accessed by is_end_zone_blkaddr() that checks the last block of a zone when f2fs is mounted as a single device.	2024-08-17	5.5	Medium
CVE-2024-43859	Linux	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to truncate preallocated blocks in f2fs_file_open() chenyuwen reports a f2fs bug as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000011 fscrypt_set_bio_crypt_ctx+0x78/0x1e8 f2fs_grab_read_bio+0x78/0x208 f2fs_submit_page_read+0x44/0x154 f2fs_get_read_data_page+0x288/0x5f4 f2fs_get_lock_data_page+0x60/0x190 truncate_partial_data_page+0x108/0x4fc f2fs_do_truncate_blocks+0x344/0x5f0 f2fs_truncate_blocks+0x6c/0x134 f2fs_truncate+0xd8/0x200 f2fs_iget+0x20c/0x5ac do_garbage_collect+0x5d0/0xf6c f2fs_gc+0x22c/0x6a4 f2fs_disable_checkpoint+0xc8/0x310 f2fs_fill_super+0x14bc/0x1764 mount_bdev+0x1b4/0x21c f2fs_mount+0x20/0x30 legacy_get_tree+0x50/0xbc vfs_get_tree+0x5c/0x1b0 do_new_mount+0x298/0x4cc path_mount+0x33c/0x5fc __arm64_sys_mount+0xcc/0x15c invoke_syscall+0x60/0x150 el0_svc_common+0xb8/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 el0t_64_sync_handler+0x88/0xec It is because inode.i_crypt_info is not initialized during below path: - mount - f2fs_fill_super - f2fs_disable_checkpoint - f2fs_gc - f2fs_iget - f2fs_truncate So, let's relocate truncation of preallocated blocks to f2fs_file_open(), after fscrypt_file_open().	2024-08-17	5.5	Medium
CVE-2024-43860	Linux	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node	2024-08-17	5.5	Medium

		value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the prescribed 70-75 charcters]			
CVE-2024-39418	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction.	2024-08-14	5.4	Medium
CVE-2024-7715	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240812. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument filter leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-13	5.3	Medium
CVE-2024-41941	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and modify settings in the application without authorization.	2024-08-13	5.3	Medium
CVE-2024-41723	F5	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	5.3	Medium
CVE-2023-50315	IBM	IBM WebSphere Application Server 8.5 and 9.0 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 274714.	2024-08-14	5.3	Medium
CVE-2024-7833	D-Link	A vulnerability was found in D-Link DI-8100 16.07. It has been classified as critical. This affects the function upgrade_filter_asp of the file upgrade_filter.asp. The manipulation of the argument path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	Medium
CVE-2024-39922	Siemens	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA1) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA1) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA1) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA1) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA1) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA1) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA1) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA1) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1) (All versions). Affected devices store user passwords in plaintext without proper protection. This could allow a physical attacker to retrieve them from the embedded storage ICs.	2024-08-13	5.1	Medium
CVE-2024-41938	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The importCertificate function of the SINEC NMS Control web application contains a path traversal vulnerability. This could allow an authenticated attacker it to delete arbitrary certificate files on the drive SINEC NMS is installed on.	2024-08-13	5.1	Medium
CVE-2024-41719	F5	When generating QKView of BIG-IP Next instance from the BIG-IP Next Central Manager (CM), F5 iHealth credentials will be logged in the BIG-IP Central Manager logs. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	5.1	Medium

CVE-2024-40704	IBM	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers. IBM X-Force ID: 298277.	2024-08-15	4.9	Medium
CVE-2023-47728	IBM	IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the request. This information could be used in further attacks against the system. IBM X-Force ID: 272201.	2024-08-16	4.9	Medium
CVE-2024-41774	IBM	IBM Common Licensing 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user 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: 350348.	2024-08-13	4.8	Medium
CVE-2022-38382	IBM	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 does not invalidate session after logout which could allow another user to obtain sensitive information. IBM X-Force ID: 233672.	2024-08-13	4.7	Medium
CVE-2024-38123	Microsoft	Windows Bluetooth Driver Information Disclosure Vulnerability	2024-08-13	4.4	Medium
CVE-2024-22114	Zabbix	User with no permission to any of the Hosts can access and view host count & other statistics through System Information Widget in Global View Dashboard.	2024-08-12	4.3	Medium
CVE-2024-39404	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39405	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39407	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39411	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39412	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39413	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39414	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39415	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39416	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-39417	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged	2024-08-14	4.3	Medium

		attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.			
CVE-2024-39419	Adobe	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	Medium
CVE-2024-38143	Microsoft	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability	2024-08-13	4.2	Medium
CVE-2024-22122	Zabbix	Zabbix allows to configure SMS notifications. AT command injection occurs on "Zabbix Server" because there is no validation of "Number" field on Web nor on Zabbix server side. Attacker can run test of SMS providing specially crafted phone number and execute additional AT commands on modem.	2024-08-12	3	Low
CVE-2024-22123	Zabbix	Setting SMS media allows to set GSM modem file. Later this file is used as Linux device. But due everything is a file for Linux, it is possible to set another file, e.g. log file and zabbix_server will try to communicate with it as modem. As a result, log file will be broken with AT commands and small part for log file content will be leaked to UI.	2024-08-12	2.7	Low
CVE-2024-41907	Siemens	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application is missing general HTTP security headers in the web server. This could allow an attacker to make the servers more prone to clickjacking attack.	2024-08-13	2.1	Low