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 ٨ سبتمبر إلى ١٤ سبتمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية 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 8th of September to 14th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-45032	Siemens	A vulnerability has been identified in Industrial Edge Management Pro (All versions < V1.9.5), Industrial Edge Management Virtual (All versions < V2.3.1-1). Affected components do not properly validate the device tokens. This could allow an unauthenticated remote attacker to impersonate other devices onboarded to the system.	2024-09-10	10	Critical
CVE-2024-38194	Microsoft	An authenticated attacker can exploit an improper authorization vulnerability in Azure Web Apps to elevate privileges over a network.	2024-09-10	9.9	Critical
CVE-2024-6342	Zyxel	**UNSUPPORTED WHEN ASSIGNED** A command injection vulnerability in the export-cgi program of Zyxel NAS326 firmware versions through V5.21(AAZF.18)C0 and NAS542 firmware versions through V5.21(ABAG.15)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	2024-09-10	9.8	Critical
CVE-2024-39581	Dell	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a File or Directories Accessible to External Parties vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to read, modify, and delete arbitrary files.	2024-09-10	9.8	Critical
CVE-2024-39583	Dell	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a Use of a Broken or Risky Cryptographic Algorithm vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	2024-09-10	9.8	Critical
CVE-2024-38225	Microsoft	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	2024-09-10	9.8	Critical
CVE-2024-38240	Microsoft	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	2024-09-10	9.8	Critical
CVE-2024-43455	Microsoft	Windows Remote Desktop Licensing Service Spoofing Vulnerability	2024-09-10	9.8	Critical
CVE-2024-43491	Microsoft	Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10, version 1507 (initial version released July 2015). This means that an attacker could exploit these previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability. This servicing stack vulnerability is addressed by installing the September 2024 Servicing stack update (SSU KB5043936) AND the September 2024 Windows security update (KB5043083), in that order. Note: Windows 10, version 1507 reached the end of support (EOS) on May 9, 2017 for devices running the Pro, Home, Enterprise, Education, and Enterprise IoT editions. Only Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB editions are still under support.	2024-09-10	9.8	Critical

CVE-2024-8191	Ivanti	SQL injection in the management console of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.	2024-09-10	9.8	Critical
CVE-2024-29847	Ivanti	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.	2024-09-12	9.8	Critical
CVE-2024-28990	SolarWinds	SolarWinds Access Rights Manager (ARM) was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability would allow access to the RabbitMQ management console. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	2024-09-12	9.8	Critical
CVE-2024-41874	Adobe	ColdFusion versions 2023.9, 2021.15 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability by providing crafted input to the application, which when deserialized, leads to execution of malicious code. Exploitation of this issue does not require user interaction.	2024-09-13	9.8	Critical
CVE-2024-35783	Siemens	A vulnerability has been identified in SIMATIC BATCH V9.1 (All versions), SIMATIC Information Server 2020 (All versions), SIMATIC Information Server 2022 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC Process Historian 2020 (All versions), SIMATIC Process Historian 2022 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 18), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5). The affected products run their DB server with elevated privileges which could allow an authenticated attacker to execute arbitrary OS commands with administrative privileges.	2024-09-10	9.4	Critical
CVE-2024-33698	Siemens	A vulnerability has been identified in SIMATIC Information Server 2022 (All versions), SIMATIC Information Server 2024 (All versions), SIMATIC PCS neo V4.0 (All versions), SIMATIC PCS neo V4.1 (All versions < V4.1 Update 2), SIMATIC PCS neo V5.0 (All versions), SINEC NMS (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions), Totally Integrated Automation Portal (TIA Portal) V19 (All versions). Affected products contain a heap-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code.	2024-09-10	9.3	Critical
CVE-2024-41171	Siemens	A vulnerability has been identified in SINUMERIK 828D V4 (All versions), SINUMERIK 828D V5 (All versions < V5.24), SINUMERIK 840D sl V4 (All versions), SINUMERIK ONE (All versions < V6.24). Affected devices do not properly enforce access restrictions to scripts that are regularly executed by the system with elevated privileges. This could allow an authenticated local attacker to escalate their privileges in the underlying system.	2024-09-10	9.3	Critical
CVE-2024-44087	Siemens	A vulnerability has been identified in Automation License Manager V5 (All versions), Automation License Manager V6.0 (All versions), Automation License Manager V6.2 (All versions < V6.2 Upd3). Affected applications do not properly validate certain fields in incoming network packets on port 4410/tcp. This could allow an unauthenticated remote attacker to cause an integer overflow and crash of the application. This denial of service condition could prevent legitimate users from using subsequent products that rely on the affected application for license verification.	2024-09-10	9.2	Critical
CVE-2024-38216	Microsoft	Azure Stack Hub Elevation of Privilege Vulnerability	2024-09-10	9	Critical
CVE-2024-38220	Microsoft	Azure Stack Hub Elevation of Privilege Vulnerability	2024-09-10	9	Critical
CVE-2024-8695	Docker	A remote code execution (RCE) vulnerability via crafted extension description/changelog could be abused by a malicious extension in Docker Desktop before 4.34.2.	2024-09-12	9	Critical
CVE-2024-8696	Docker	A remote code execution (RCE) vulnerability via crafted extension publisher-url/additional-urls could be abused by a malicious extension in Docker Desktop before 4.34.2.	2024-09-12	8.9	High
CVE-2024-26186	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-26191	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-37335	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-37338	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High

CVE-2024-37339	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-37340	Microsoft	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-37341	Microsoft	Microsoft SQL Server Elevation of Privilege Vulnerability	2024-09-10	8.8	High
CVE-2024-37965	Microsoft	Microsoft SQL Server Elevation of Privilege Vulnerability	2024-09-10	8.8	High
CVE-2024-37980	Microsoft	Microsoft SQL Server Elevation of Privilege Vulnerability	2024-09-10	8.8	High
CVE-2024-38018	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-38259	Microsoft	Microsoft Management Console Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-38260	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-43461	Microsoft	Windows MSHTML Platform Spoofing Vulnerability	2024-09-10	8.8	High
CVE-2024-43469	Microsoft	Azure CycleCloud Remote Code Execution Vulnerability	2024-09-10	8.8	High
CVE-2024-8322	Ivanti	Weak authentication in Patch Management of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker to access restricted functionality.	2024-09-10	8.8	High
CVE-2024-8636	Google	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-11	8.8	High
CVE-2024-8637	Google	Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-11	8.8	High
CVE-2024-8638	Google	Type Confusion in V8 in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-11	8.8	High
CVE-2024-8639	Google	Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-11	8.8	High
CVE-2024-20381	Cisco	A vulnerability in the JSON-RPC API feature in ConfD that is used by the web-based management interfaces of Cisco Crosswork Network Services Orchestrator (NSO), Cisco Optical Site Manager, and Cisco RV340 Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to modify the configuration of an affected application or device. This vulnerability is due to improper authorization checks on the API. An attacker with privileges sufficient to access the affected application or device could exploit this vulnerability by sending malicious requests to the JSON-RPC API. A successful exploit could allow the attacker to make unauthorized modifications to the configuration of the affected application or device, including creating new user accounts or elevating their own privileges on an affected system.	2024-09-11	8.8	High
CVE-2024-20398	Cisco	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to obtain read/write file system access on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user arguments that are passed to specific CLI commands. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the prompt. A successful exploit could allow the attacker to elevate privileges to root.	2024-09-11	8.8	High
CVE-2024-28991	SolarWinds	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a remote code execution vulnerability. If exploited, this vulnerability would allow an authenticated user to abuse the service, resulting in remote code execution.	2024-09-12	8.8	High
CVE-2024-43647	Siemens	A vulnerability has been identified in SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-	2024-09-10	8.7	High

		0AA0) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) (All versions). Affected devices do not properly handle TCP packets with an incorrect structure. This could allow an unauthenticated remote attacker to cause a denial of service condition. To restore normal operations, the network cable of the device needs to be unplugged and re-plugged.			
CVE-2024-8321	Ivanti	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to isolate managed devices from the network.	2024-09-10	8.6	High
CVE-2024-20304	Cisco	A vulnerability in the multicast traceroute version 2 (Mtrace2) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to exhaust the UDP packet memory of an affected device. This vulnerability exists because the Mtrace2 code does not properly handle packet memory. An attacker could exploit this vulnerability by sending crafted packets to an affected device. A successful exploit could allow the attacker to exhaust the incoming UDP packet memory. The affected device would not be able to process higher-level UDP-based protocols packets, possibly causing a denial of service (DoS) condition. Note: This vulnerability can be exploited using IPv4 or IPv6.	2024-09-11	8.6	High
CVE-2024-43479	Microsoft	Microsoft Power Automate Desktop Remote Code Execution Vulnerability	2024-09-10	8.5	High
CVE-2024-31336	Google	In PVRSRVBridgeRGXKickTA3D2 of server_rgxta3d_bridge.c, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	8.4	High
CVE-2024-20489	Cisco	A vulnerability in the storage method of the PON Controller configuration file could allow an authenticated, local attacker with low privileges to obtain the MongoDB credentials. This vulnerability is due to improper storage of the unencrypted database credentials on the device that is running Cisco IOS XR Software. An attacker could exploit this vulnerability by accessing the configuration files on an affected system. A successful exploit could allow the attacker to view MongoDB credentials.	2024-09-11	8.4	High
CVE-2023-28827	Siemens	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle certain requests, causing a timeout in the watchdog, which could lead to the clean up of pointers. This could allow a remote attacker to cause a denial of service condition in the system.	2024-09-10	8.2	High
CVE-2023-30756	Siemens	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC	2024-09-10	8.2	High

		(6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle certain errors when using the Expect HTTP request header, resulting in NULL dereference. This could allow a remote attacker with no privileges to cause a denial of service condition in the system.			
CVE-2024-37397	Ivanti	An External XML Entity (XXE) vulnerability in the provisioning web service of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to leak API secrets.	2024-09-12	8.2	High
CVE-2024-21416	Microsoft	Windows TCP/IP Remote Code Execution Vulnerability	2024-09-10	8.1	High
CVE-2024-38045	Microsoft	Windows TCP/IP Remote Code Execution Vulnerability	2024-09-10	8.1	High
CVE-2024-30073	Microsoft	Windows Security Zone Mapping Security Feature Bypass Vulnerability	2024-09-10	7.8	High
CVE-2024-38014	Microsoft	Windows Installer Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38046	Microsoft	PowerShell Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38237	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38238	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38241	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38242	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38243	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38244	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38245	Microsoft	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38247	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38249	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38250	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38252	Microsoft	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-38253	Microsoft	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-43457	Microsoft	Windows Setup and Deployment Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-43463	Microsoft	Microsoft Office Visio Remote Code Execution Vulnerability	2024-09-10	7.8	High
CVE-2024-43465	Microsoft	Microsoft Excel Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-43492	Microsoft	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	2024-09-10	7.8	High
CVE-2024-44103	Ivanti	DLL hijacking in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	2024-09-10	7.8	High
CVE-2024-44104	Ivanti	An incorrectly implemented authentication scheme that is subjected to a spoofing attack in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	2024-09-10	7.8	High
CVE-2024-44105	Ivanti	Cleartext transmission of sensitive information in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to obtain OS credentials.	2024-09-10	7.8	High
CVE-2024-44106	Ivanti	Insufficient server-side controls in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	2024-09-10	7.8	High
CVE-2024-44107	Ivanti	DLL hijacking in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges and achieve arbitrary code execution.	2024-09-10	7.8	High
CVE-2024-8012	Ivanti	An authentication bypass weakness in the message broker service of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	2024-09-10	7.8	High
CVE-2024-40650	Google	In wifi_item_edit_content of styles.xml , there is a possible FRP bypass due to Missing check for FRP state. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	7.8	High
CVE-2024-40655	Google	In bindAndGetCallIdentification of CallScreeningServiceHelper.java, there is a possible way to maintain a while-in-use permission in the background due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-09-11	7.8	High
CVE-2024-40657	Google	In addPreferencesForType of AccountTypePreferenceLoader.java, there is a possible way to disable apps for other users due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	7.8	High
CVE-2024-40658	Google	In getConfig of SoftVideoDecoderOMXComponent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	7.8	High

CVE-2024-40662	Google	In scheme of Uri.java, there is a possible way to craft a malformed Uri object due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	7.8	High
CVE-2024-39378	Adobe	Audition versions 24.4.1, 23.6.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-09-11	7.8	High
CVE-2024-45026	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case.	2024-09-11	7.8	High
CVE-2024-46673	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free.	2024-09-13	7.8	High
CVE-2024-46674	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources.	2024-09-13	7.8	High
CVE-2024-46683	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: prevent UAF around preempt fence The fence lock is part of the queue, therefore in the current design anything locking the fence should then also hold a ref to the queue to prevent the queue from being freed. However, currently it looks like we signal the fence and then drop the queue ref, but if something is waiting on the fence, the waiter is kicked to wake up at some later point, where upon waking up it first grabs the lock before checking the fence state. But if we have	2024-09-13	7.8	High

		already dropped the queue ref, then the lock might already be freed as part of the queue, leading to uaf. To prevent this, move the fence lock into the fence itself so we don't run into lifetime issues. Alternative might be to have device level lock, or only release the queue in the fence release callback, however that might require pushing to another worker to avoid locking issues. References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2454 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2342 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2020 (cherry picked from commit 7116c35aacedc38be6d15bd21b2fc936eed0008b)			
CVE-2024-46687	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix a use-after-free when hitting errors inside btrfs_submit_chunk() [BUG] There is an internal report that KASAN is reporting use-after-free, with the following backtrace: BUG: KASAN: slab-use-after-free in btrfs_check_read_bio+0xa68/0xb70 [btrfs] Read of size 4 at addr ffff8881117cec28 by task kworker/u16:2/45 CPU: 1 UID: 0 PID: 45 Comm: kworker/u16:2 Not tainted 6.11.0-rc2-next-20240805-default+ #76 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 Workqueue: btrfs-endio btrfs_end_bio_work [btrfs] Call Trace: dump_stack_lvl+0x61/0x80 print_address_description.constprop.0+0x5e/0x2f0 print_report+0x118/0x216 kasan_report+0x11d/0x1f0 btrfs_check_read_bio+0xa68/0xb70 [btrfs] process_one_work+0xce0/0x12a0 worker_thread+0x717/0x1250 kthread+0x2e3/0x3c0 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 Allocated by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 __kasan_slab_alloc+0x7d/0x80 kmem_cache_alloc_noprof+0x16e/0x3e0 mempool_alloc_noprof+0x12e/0x310 bio_alloc_bioset+0x3f0/0x7a0 btrfs_bio_alloc+0x2e/0x50 [btrfs] submit_extent_page+0x4d1/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x4b/0x60 kmem_cache_free+0x214/0x5d0 bio_free+0xed/0x180 end_bbio_data_read+0x1cc/0x580 [btrfs]	2024-09-13	7.8	High

		btrfs_submit_chunk+0x98d/0x1880 [btrfs] btrfs_submit_bio+0x33/0x70 [btrfs] submit_one_bio+0xd4/0x130 [btrfs] submit_extent_page+0x3ea/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [CAUSE] Although I cannot reproduce the error, the report itself is good enough to pin down the cause. The call trace is the regular endio workqueue context, but the free-by-task trace is showing that during btrfs_submit_chunk() we already hit a critical error, and is calling btrfs_bio_end_io() to error out. And the original endio function called bio_put() to free the whole bio. This means a double freeing thus causing use-after-free, e.g.: 1. Enter btrfs_submit_bio() with a read bio The read bio length is 128K, crossing two 64K stripes. 2. The first run of btrfs_submit_chunk() 2.1 Call btrfs_map_block(), which returns 64K 2.2 Call btrfs_split_bio() Now there are two bios, one referring to the first 64K, the other referring to the second 64K. 2.3 The first half is submitted. 3. The second run of btrfs_submit_chunk() 3.1 Call btrfs_map_block(), which by somehow failed Now we call btrfs_bio_end_io() to handle the error 3.2 btrfs_bio_end_io() calls the original endio function Which is end_bbio_data_read(), and it calls bio_put() for the original bio. Now the original bio is freed. 4. The submitted first 64K bio finished Now we call into btrfs_check_read_bio() and tries to advance the bio iter. But since the original bio (thus its iter) is already freed, we trigger the above use-after free. And even if the memory is not poisoned/corrupted, we will later call the original endio function, causing a double freeing. [FIX] Instead of calling btrfs_bio_end_io(), call btrfs_orig_bbio_end_io(), which has the extra check on split bios and do the pr ---truncated---			
CVE-2024-46696	Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix potential UAF in nfsd4_cb_getattr_release Once we drop the delegation reference, the fields embedded in it are no longer safe to access. Do that last.	2024-09-13	7.8	High
CVE-2024-46699	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Disable preemption while updating GPU stats We forgot to disable preemption around the write_seqcount_begin/end() pair while updating GPU stats:	2024-09-13	7.8	High

		[ ] WARNING: CPU: 2 PID: 12 at include/linux/seqlock.h:221 __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] Workqueue: v3d_bin drm_sched_run_job_work [gpu_sched] <...snip...> [ ] Call trace: [ ] __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] v3d_job_start_stats.isra.0+0x90/0x218 [v3d] [ ] v3d_bin_job_run+0x23c/0x388 [v3d] [ ] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [ ] process_one_work+0x62c/0xb48 [ ] worker_thread+0x468/0x5b0 [ ] kthread+0x1c4/0x1e0 [ ] ret_from_fork+0x10/0x20 Fix it.			
CVE-2024-46700	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/mes: fix mes ring buffer overflow wait memory room until enough before writing mes packets to avoid ring buffer overflow. v2: squash in sched_hw_submission fix (cherry picked from commit 34e087e8920e635c62e2ed6a758b0cd27f836d13)	2024-09-13	7.8	High
CVE-2024-39377	Adobe	Media Encoder versions 24.5, 23.6.8 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.	2024-09-13	7.8	High
CVE-2024-41871	Adobe	Media Encoder versions 24.5, 23.6.8 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.	2024-09-13	7.8	High
CVE-2024-34121	Adobe	Illustrator versions 28.6, 27.9.5 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.	2024-09-13	7.8	High
CVE-2024-39380	Adobe	After Effects versions 23.6.6, 24.5 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.	2024-09-13	7.8	High
CVE-2024-39381	Adobe	After Effects versions 23.6.6, 24.5 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.	2024-09-13	7.8	High
CVE-2024-39384	Adobe	Premiere Pro versions 24.5, 23.6.8 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.	2024-09-13	7.8	High
CVE-2024-41857	Adobe	Illustrator versions 28.6, 27.9.5 and earlier are affected by an Integer Underflow (Wrap 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.	2024-09-13	7.8	High
CVE-2024-41859	Adobe	After Effects versions 23.6.6, 24.5 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.	2024-09-13	7.8	High
CVE-2024-41869	Adobe	Acrobat Reader versions 24.002.21005, 24.001.30159, 20.005.30655, 24.003.20054 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.	2024-09-13	7.8	High
CVE-2024-43758	Adobe	Illustrator versions 28.6, 27.9.5 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	2024-09-13	7.8	High

		issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-45112	Adobe	Acrobat Reader versions 24.002.21005, 24.001.30159, 20.005.30655, 24.003.20054 and earlier are affected by a Type Confusion vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when a resource is accessed using a type that is not compatible with the actual object type, leading to a logic error that an attacker could exploit. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-09-13	7.8	High
CVE-2024-43756	Adobe	Photoshop Desktop versions 24.7.4, 25.11 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.	2024-09-13	7.8	High
CVE-2024-43760	Adobe	Photoshop Desktop versions 24.7.4, 25.11 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 issue requires user interaction in that a victim must open a malicious file.	2024-09-13	7.8	High
CVE-2024-45108	Adobe	Photoshop Desktop versions 24.7.4, 25.11 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 issue requires user interaction in that a victim must open a malicious file.	2024-09-13	7.8	High
CVE-2024-45109	Adobe	Photoshop Desktop versions 24.7.4, 25.11 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 issue requires user interaction in that a victim must open a malicious file.	2024-09-13	7.8	High
CVE-2024-29779	Google	there is a possible escalation of privilege due to an unusual root cause. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-13	7.8	High
CVE-2024-44092	Google	In TBD of TBD, there is a possible LCS signing enforcement missing due to test/debugging code left in a production build. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-13	7.8	High
CVE-2024-44093	Google	In ppmp_unprotect_buf of drm/code/drm_fw.c, there is a possible memory corruption 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.	2024-09-13	7.8	High
CVE-2024-44094	Google	In ppmp_protect_mfcfw_buf of code/drm_fw.c, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-13	7.8	High
CVE-2024-44095	Google	In ppmp_protect_mfcfw_buf of code/drm_fw.c, there is a possible corrupt memory 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.	2024-09-13	7.8	High
CVE-2024-43458	Microsoft	Windows Networking Information Disclosure Vulnerability	2024-09-10	7.7	High
CVE-2024-42427	Dell	Dell ThinOS versions 2402 and 2405, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Elevation of privileges.	2024-09-10	7.6	High
CVE-2024-43474	Microsoft	Microsoft SQL Server Information Disclosure Vulnerability	2024-09-10	7.6	High
CVE-2024-38119	Microsoft	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability	2024-09-10	7.5	High
CVE-2024-38230	Microsoft	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-38231	Microsoft	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-38232	Microsoft	Windows Networking Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-38233	Microsoft	Windows Networking Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-38236	Microsoft	DHCP Server Service Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-38257	Microsoft	Microsoft AllJoyn API Information Disclosure Vulnerability	2024-09-10	7.5	High
CVE-2024-38258	Microsoft	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability	2024-09-10	7.5	High
CVE-2024-38263	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-09-10	7.5	High
CVE-2024-43466	Microsoft	Microsoft SharePoint Server Denial of Service Vulnerability	2024-09-10	7.5	High
CVE-2024-43467	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-09-10	7.5	High
CVE-2024-45327	Fortinet	An improper authorization vulnerability [CWE-285] in FortiSOAR version 7.4.0 through 7.4.3, 7.3.0 through 7.3.2, 7.2.0 through 7.2.2, 7.0.0 through 7.0.3 change password endpoint may allow an authenticated attacker to perform a brute force attack on users and administrators password via crafted HTTP requests.	2024-09-11	7.5	High

CVE-2024-45113	Adobe	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access and affect the integrity of the application. Exploitation of this issue does not require user interaction.	2024-09-13	7.5	High
CVE-2024-23716	Google	In DevmemIntPFNotify of devicemem_server.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-09-11	7.4	High
CVE-2024-20317	Cisco	A vulnerability in the handling of specific Ethernet frames by Cisco IOS XR Software for various Cisco Network Convergence System (NCS) platforms could allow an unauthenticated, adjacent attacker to cause critical priority packets to be dropped, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect classification of certain types of Ethernet frames that are received on an interface. An attacker could exploit this vulnerability by sending specific types of Ethernet frames to or through the affected device. A successful exploit could allow the attacker to cause control plane protocol relationships to fail, resulting in a DoS condition. For more information, see the section of this advisory. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-09-11	7.4	High
CVE-2024-20406	Cisco	A vulnerability in the segment routing feature for the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of ingress IS-IS packets. An attacker could exploit this vulnerability by sending specific IS-IS packets to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the IS-IS process on all affected devices that are participating in the Flexible Algorithm to crash and restart, resulting in a DoS condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2-adjacent to the affected device and must have formed an adjacency. This vulnerability affects segment routing for IS-IS over IPv4 and IPv6 control planes as well as devices that are configured as level 1, level 2, or multi-level routing IS-IS type.	2024-09-11	7.4	High
CVE-2024-41170	Siemens	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0015), Tecnomatix Plant Simulation V2404 (All versions < V2404.0004). The affected applications contain a stack based overflow vulnerability while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	2024-09-10	7.3	High
CVE-2024-33508	Fortinet	An improper neutralization of special elements used in a command ('Command Injection') vulnerability [CWE-77] in Fortinet FortiClientEMS 7.2.0 through 7.2.4, 7.0.0 through 7.0.12 may allow an unauthenticated attacker to execute limited and temporary operations on the underlying database via crafted requests.	2024-09-10	7.3	High
CVE-2024-38226	Microsoft	Microsoft Publisher Security Feature Bypass Vulnerability	2024-09-10	7.3	High
CVE-2024-43470	Microsoft	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	2024-09-10	7.3	High
CVE-2024-43475	Microsoft	Microsoft Windows Admin Center Information Disclosure Vulnerability	2024-09-10	7.3	High
CVE-2024-43495	Microsoft	Windows libarchive Remote Code Execution Vulnerability	2024-09-10	7.3	High
CVE-2024-40652	Google	In onCreate of SettingsHomepageActivity.java, there is a possible way to access the Settings app while the device is provisioning due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-09-11	7.3	High
CVE-2024-20430	Cisco	A vulnerability in Cisco Meraki Systems Manager (SM) Agent for Windows could allow an authenticated, local attacker to execute arbitrary code with elevated privileges. This vulnerability is due to incorrect handling of directory search paths at runtime. A low-privileged attacker could exploit this	2024-09-12	7.3	High

		vulnerability by placing both malicious configuration files and malicious DLL files on an affected system, which would read and execute the files when Cisco Meraki SM launches on startup. A successful exploit could allow the attacker to execute arbitrary code on the affected system with SYSTEM privileges.			
CVE-2024-38227	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-09-10	7.2	High
CVE-2024-38228	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-09-10	7.2	High
CVE-2024-38239	Microsoft	Windows Kerberos Elevation of Privilege Vulnerability	2024-09-10	7.2	High
CVE-2024-43464	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-09-10	7.2	High
CVE-2024-8190	Ivanti	An OS command injection vulnerability in Ivanti Cloud Services Appliance versions 4.6 Patch 518 and before allows a remote authenticated attacker to obtain remote code execution. The attacker must have admin level privileges to exploit this vulnerability.	2024-09-10	7.2	High
CVE-2024-20483	Cisco	Multiple vulnerabilities in Cisco Routed PON Controller Software, which runs as a docker container on hardware that is supported by Cisco IOS XR Software, could allow an authenticated, remote attacker with Administrator-level privileges on the PON Manager or direct access to the PON Manager MongoDB instance to perform command injection attacks on the PON Controller container and execute arbitrary commands as root. These vulnerabilities are due to insufficient validation of arguments that are passed to specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input as the argument of an affected configuration command. A successful exploit could allow the attacker to execute arbitrary commands as root on the PON controller.	2024-09-11	7.2	High
CVE-2024-32840	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-32842	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-32843	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-32845	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-32846	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-32848	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-34779	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-34783	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-34785	Ivanti	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-09-12	7.2	High
CVE-2024-8278	Lenovo	A privilege escalation vulnerability was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection via specially crafted IPMI commands.	2024-09-13	7.2	High
CVE-2024-8279	Lenovo	A privilege escalation vulnerability was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	2024-09-13	7.2	High
CVE-2024-8280	Lenovo	An input validation weakness was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection or cause a recoverable denial of service using a specially crafted file.	2024-09-13	7.2	High
CVE-2024-8281	Lenovo	An input validation weakness was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection through specially crafted command line input in the XCC SSH captive shell.	2024-09-13	7.2	High
CVE-2024-37337	Microsoft	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	2024-09-10	7.1	High
CVE-2024-37342	Microsoft	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	2024-09-10	7.1	High
CVE-2024-37966	Microsoft	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	2024-09-10	7.1	High

CVE-2024-38188	Microsoft	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	2024-09-10	7.1	High
CVE-2024-43454	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-09-10	7.1	High
CVE-2024-45023	Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid1: Fix data corruption for degraded array with slow disk read_balance() will avoid reading from slow disks as much as possible, however, if valid data only lands in slow disks, and a new normal disk is still in recovery, unrecovered data can be read: raid1_read_request read_balance raid1_should_read_first -> return false choose_best_rdev -> normal disk is not recovered, return -1 choose_bb_rdev -> missing the checking of recovery, return the normal disk -> read unrecovered data Root cause is that the checking of recovery is missing in choose_bb_rdev(). Hence add such checking to fix the problem. Also fix similar problem in choose_slow_rdev().	2024-09-11	7.1	High
CVE-2024-37990	Siemens	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected applications contain configuration files which can be modified. An attacker with privilege access can modify these files and enable features that are not released for this device.	2024-09-10	7	High
CVE-2024-38246	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-09-10	7	High
CVE-2024-38248	Microsoft	Windows Storage Elevation of Privilege Vulnerability	2024-09-10	7	High
CVE-2024-7889	Citrix	Local privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	2024-09-11	7	High
CVE-2023-49069	Siemens	A vulnerability has been identified in Mendix Runtime V10 (All versions < V10.14.0 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.12 (All versions < V10.12.2 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.6 (All versions < V10.6.12 only if the basic authentication mechanism is used by the application), Mendix Runtime V8 (All versions < V8.18.31 only if the basic authentication mechanism is used by the application), Mendix Runtime V9 (All versions < V9.24.26 only if the basic authentication mechanism is used by the application). The authentication mechanism of affected applications contains an observable response discrepancy vulnerability when validating usernames. This could allow unauthenticated remote attackers to distinguish between valid and invalid usernames.	2024-09-10	6.9	Medium

		A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected applications do not authenticated the creation of Ajax2App instances. This could allow an unauthenticated attacker to cause a denial of service condition.			
CVE-2024-37993	Siemens		2024-09-10	6.9	Medium
		A vulnerability has been identified in SINUMERIK 828D V4 (All versions < V4.95 SP3), SINUMERIK 840D sl V4 (All versions < V4.95 SP3 in connection with using Create MyConfig (CMC) <= V4.8 SP1 HF6), SINUMERIK ONE (All versions < V6.23 in connection with using Create MyConfig (CMC) <= V6.6), SINUMERIK ONE (All versions < V6.15 SP4 in connection with using Create MyConfig (CMC) <= V6.6). Affected systems, that have been provisioned with Create MyConfig (CMC), contain a Insertion of Sensitive Information into Log File vulnerability. This could allow a local authenticated user with low privileges to read sensitive information and thus circumvent access restrictions.			
CVE-2024-43781	Siemens		2024-09-10	6.8	Medium
		AAn improper certificate validation vulnerability [CWE-295] in FortiClientWindows 7.2.0 through 7.2.2, 7.0.0 through 7.0.11, FortiClientLinux 7.2.0, 7.0.0 through 7.0.11 and FortiClientMac 7.0.0 through 7.0.11, 7.2.0 through 7.2.4 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the FortiGate and the FortiClient during the ZTNA tunnel creation			
CVE-2024-31489	Fortinet		2024-09-10	6.8	Medium
		A privilege escalation vulnerability was discovered when Single Sign On (SSO) is enabled that could allow an attacker to intercept a valid, authenticated LXCA user's XCC session if they can convince the user to click on a specially crafted URL.			
CVE-2024-45101	Lenovo		2024-09-13	6.8	Medium
		A potential vulnerability was reported in the ThinkPad L390 Yoga and 10w Notebook that could allow a local attacker to escalate privileges by accessing an embedded UEFI shell.			
CVE-2024-7756	Lenovo		2024-09-13	6.8	Medium
		Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains an Improper Access Control vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.			
CVE-2024-39580	Dell		2024-09-10	6.7	Medium
		An uncontrolled search path in the agent of Ivanti EPM before 2022 SU6, or the 2024 September update allows a local authenticated attacker with admin privileges to escalate their privileges to SYSTEM.			
CVE-2024-8441	Ivanti		2024-09-10	6.7	Medium
		A potential buffer overflow vulnerability was reported in some Lenovo Notebook products that could allow a local attacker with elevated privileges to execute arbitrary code.			
CVE-2024-3100	Lenovo		2024-09-13	6.7	Medium
		An internal product security audit discovered a UEFI SMM (System Management Mode) callout vulnerability in some ThinkSystem servers that could allow a local attacker with elevated privileges to execute arbitrary code.			
CVE-2024-45105	Lenovo		2024-09-13	6.7	Medium
		A potential buffer overflow vulnerability was reported in some Lenovo ThinkSystem and ThinkStation products that could allow a local attacker with elevated privileges to execute arbitrary code.			
CVE-2024-4550	Lenovo		2024-09-13	6.7	Medium
		An insufficient entropy vulnerability caused by the improper use of a randomness function with low entropy for web authentication tokens generation exists in the Zyxel GS1900-10HP firmware			
CVE-2024-38270	Zyxel		2024-09-10	6.5	Medium

		version V2.80(AAZI.0)C0. This vulnerability could allow a LAN-based attacker a slight chance to gain a valid session token if multiple authenticated sessions are alive.			
CVE-2024-38234	Microsoft	Windows Networking Denial of Service Vulnerability	2024-09-10	6.5	Medium
CVE-2024-38235	Microsoft	Windows Hyper-V Denial of Service Vulnerability	2024-09-10	6.5	Medium
CVE-2024-43482	Microsoft	Microsoft Outlook for iOS Information Disclosure Vulnerability	2024-09-10	6.5	Medium
CVE-2024-43487	Microsoft	Windows Mark of the Web Security Feature Bypass Vulnerability	2024-09-10	6.5	Medium
CVE-2024-38222	Microsoft	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-09-12	6.5	Medium
CVE-2024-45104	Lenovo	A valid, authenticated LXCA user without sufficient privileges may be able to use the device identifier to modify an LXCA managed device through a specially crafted web API call.	2024-09-13	6.5	Medium
CVE-2024-38254	Microsoft	Windows Authentication Information Disclosure Vulnerability	2024-09-10	6.2	Medium
CVE-2024-42423	Dell	Citrix Workspace App version 23.9.0.24.4 on Dell ThinOS 2311 contains an Incorrect Authorization vulnerability when Citrix CEB is enabled for WebLogin. A local unauthenticated user with low privileges may potentially exploit this vulnerability to bypass existing controls and perform unauthorized actions leading to information disclosure and tampering.	2024-09-10	6.1	Medium
CVE-2024-37991	Siemens	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The service log files of the affected application can be accessed without proper authentication. This could allow an unauthenticated attacker to get access to sensitive information.	2024-09-10	6	Medium
CVE-2023-30755	Siemens	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle the shutdown or reboot request, which could lead to the clean up of certain resources. This could allow a remote attacker with elevated privileges to cause a denial of service condition in the system.	2024-09-10	5.9	Medium
CVE-2024-37992	Siemens	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC	2024-09-10	5.9	Medium

		(6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected devices does not properly handle the error in case of exceeding characters while setting SNMP leading to the restart of the application.			
CVE-2024-42425	Dell	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-09-10	5.5	Medium
CVE-2024-21753	Fortinet	A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiClientEMS versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.13, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8, 1.2.1 through 1.2.5 allows attacker to perform a denial of service, read or write a limited number of files via specially crafted HTTP requests	2024-09-10	5.5	Medium
CVE-2024-38256	Microsoft	Windows Kernel-Mode Driver Information Disclosure Vulnerability	2024-09-10	5.5	Medium
CVE-2024-41868	Adobe	Audition versions 24.4.1, 23.6.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-09-11	5.5	Medium
CVE-2024-45009	Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ... WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR. A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR.	2024-09-11	5.5	Medium
CVE-2024-45010	Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ... WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest from the	2024-09-11	5.5	Medium

		mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal' endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this ID is currently available, because the subflow could have been closed before.			
CVE-2024-45011	Linux	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints.	2024-09-11	5.5	Medium
CVE-2024-45012	Linux	In the Linux kernel, the following vulnerability has been resolved: nouveau/firmware: use dma non-coherent allocator Currently, enabling SG_DEBUG in the kernel will cause nouveau to hit a BUG() on startup, when the iommu is enabled: kernel BUG at include/linux/scatterlist.h:187! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 7 PID: 930 Comm: (udev-worker) Not tainted 6.9.0-rc3Lyude-Test+ #30 Hardware name: MSI MS-7A39/A320M GAMING PRO (MS-7A39), BIOS 1.I0 01/22/2019 RIP: 0010:sg_init_one+0x85/0xa0 Code: 69 88 32 01 83 e1 03 f6 c3 03 75 20 a8 01 75 1e 48 09 cb 41 89 54 24 08 49 89 1c 24 41 89 6c 24 0c 5b 5d 41 5c e9 7b b9 88 00 <0f> 0b 0f 0b 0f 0b 48 8b 05 5e 46 9a 01 eb b2 66 66 2e 0f 1f 84 00 RSP: 0018:ffffa776017bf6a0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffffa77600d87000 RCX: 000000000000002b RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffffa77680d87000 RBP: 000000000000e000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff98f4c46aa508 R11: 0000000000000000 R12: ffff98f4c46aa508 R13: ffff98f4c46aa008 R14: ffffa77600d4a000 R15: ffffa77600d4a018 FS: 00007feeb5aae980(0000) GS:ffff98f5c4dc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f22cb9a4520 CR3: 00000001043ba000 CR4: 00000000003506f0	2024-09-11	5.5	Medium

		Call Trace: <TASK> ? die+0x36/0x90 ? do_trap+0xdd/0x100 ? sg_init_one+0x85/0xa0 ? do_error_trap+0x65/0x80 ? sg_init_one+0x85/0xa0 ? exc_invalid_op+0x50/0x70 ? sg_init_one+0x85/0xa0 ? asm_exc_invalid_op+0x1a/0x20 ? sg_init_one+0x85/0xa0 nvkm_firmware_ctor+0x14a/0x250 [nouveau] nvkm_falcon_fw_ctor+0x42/0x70 [nouveau] ga102_gsp_booter_ctor+0xb4/0x1a0 [nouveau] r535_gsp_oneinit+0xb3/0x15f0 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? nvkm_udevice_new+0x95/0x140 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? ktime_get+0x47/0xb0 Fix this by using the non-coherent allocator instead, I think there might be a better answer to this, but it involve ripping up some of APIs using sg lists.			
CVE-2024-45013	Linux	In the Linux kernel, the following vulnerability has been resolved: nvme: move stopping keep-alive into nvme_uninit_ctrl() Commit 4733b65d82bd ("nvme: start keep-alive after admin queue setup") moves starting keep-alive from nvme_start_ctrl() into nvme_init_ctrl_finish(), but don't move stopping keep-alive into nvme_uninit_ctrl(), so keep-alive work can be started and keep pending after failing to start controller, finally use-after-free is triggered if nvme host driver is unloaded. This patch fixes kernel panic when running nvme/004 in case that connection failure is triggered, by moving stopping keep-alive into nvme_uninit_ctrl(). This way is reasonable because keep-alive is now started in nvme_init_ctrl_finish().	2024-09-11	5.5	Medium
CVE-2024-45014	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/boot: Avoid possible physmem_info segment corruption When physical memory for the kernel image is allocated it does not consider extra memory required for offsetting the image start to match it with the lower 20 bits of KASLR virtual base address. That might lead to kernel access beyond its memory range.	2024-09-11	5.5	Medium
CVE-2024-45015	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: move dpu_encoder's connector assignment to atomic_enable() For cases where the crtc's connectors_changed was set without enable/active getting toggled , there is an atomic_enable() call followed by an atomic_disable() but without an atomic_mode_set(). This results in a NULL ptr access for the dpu_encoder_get_drm_fmt() call in the atomic_enable() as the dpu_encoder's connector was cleared in the atomic_disable() but not re-assigned as there was no atomic_mode_set() call. Fix the NULL ptr access by moving the assignment for atomic_enable() and also use drm_atomic_get_new_connector_for_encoder() to get the connector from the atomic_state. Patchwork: https://patchwork.freedesktop.org/patch/606729/	2024-09-11	5.5	Medium
CVE-2024-45016	Linux	In the Linux kernel, the following vulnerability has been resolved:	2024-09-11	5.5	Medium

		netem: fix return value if duplicate enqueue fails
		
		There is a bug in netem_enqueue() introduced by
		commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec")
		that can lead to a use-after-free.
		
		This commit made netem_enqueue() always return NET_XMIT_SUCCESS
		when a packet is duplicated, which can cause the parent qdisc's q.qlen
		to be mistakenly incremented. When this happens qlen_notify() may be
		skipped on the parent during destruction, leaving a dangling pointer
		for some classful qdiscs like DRR.
		
		There are two ways for the bug happen:
		
		- If the duplicated packet is dropped by rootq->enqueue() and then
		  the original packet is also dropped.
		- If rootq->enqueue() sends the duplicated packet to a different qdisc
		  and the original packet is dropped.
		
		In both cases NET_XMIT_SUCCESS is returned even though no packets
		are enqueued at the netem qdisc.
		
		The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS.			

CVE-2024-45017	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix IPsec RoCE MPV trace call Prevent the call trace below from happening, by not allowing IPsec creation over a slave, if master device doesn't support IPsec. WARNING: CPU: 44 PID: 16136 at kernel/locking/rwsem.c:240 down_read+0x75/0x94 Modules linked in: esp4_offload esp4 act_mirred act_vlan cls_flower sch_ingress mlx5_vdpa vringh vhost_iotlb vdpa mst_pciconf(OE) nfsv3 nfs_acl nfs lockd grace fscache netfs xt_CHECKSUM xt_MASQUERADE xt_conntrack ipt_REJECT nf_reject_ipv4 nft_compat nft_counter nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 rfkill cuse fuse rpcrdma sunrpc rdma_ucm ib_srpt ib_isert iscsi_target_mod target_core_mod ib_umad ib_iser libiscsi scsi_transport_iscsi rdma_cm ib_ipoib iw_cm ib_cm ipmi_ssif intel_rapl_msr intel_rapl_common amd64_edac edac_mce_amd kvm_amd kvm irqbypass crct10dif_pclmul crc32_pclmul mlx5_ib ghash_clmulni_intel sha1_ssse3 dell_smbios ib_uverbs aesni_intel crypto_simd dcdbas wmi_bmof dell_wmi_descriptor cryptd pcspkr ib_core acpi_ipmi sp5100_tco ccp i2c_piix4 ipmi_si ptdma k10temp ipmi_devintf ipmi_msghandler acpi_power_meter acpi_cpufreq ext4 mbcache jbd2 sd_mod t10_pi sg mgag200 drm_kms_helper syscopyarea sysfillrect mlx5_core sysimgblt fb_sys_fops cec ahci libahci mlxfw drm pci_hyperv_intf libata tg3 sha256_ssse3 tls megaraid_sas i2c_algo_bit psample wmi dm_mirror dm_region_hash dm_log dm_mod [last unloaded: mst_pci] CPU: 44 PID: 16136 Comm: kworker/44:3 Kdump: loaded Tainted: GOE 5.15.0-20240509.el8uek.uek7_u3_update_v6.6_ipsec_bf.x86_64 #2 Hardware name: Dell Inc. PowerEdge R7525/074H08, BIOS 2.0.3 01/15/2021 Workqueue: events xfrm_state_gc_task RIP: 0010:down_read+0x75/0x94 Code: 00 48 8b 45 08 65 48 8b 14 25 80 fc 01 00 83 e0 02 48 09 d0 48 83 c8 01 48 89 45 08 5d 31 c0 89 c2 89 c6 89 c7 e9 cb 88 3b 00 <0f> 0b 48 8b 45 08 a8 01 74 b2 a8 02 75 ae 48 89 c2 48 83 ca 02 f0 RSP: 0018:ffffb26387773da8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffffa08b658af900 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ff886bc5e1366f2f RDI: 0000000000000000 RBP: ffffa08b658af940 R08: 0000000000000000 R09:	2024-09-11	5.5	Medium

		0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffa0a9bfb31540 R13: ffffa0a9bfb37900 R14: 0000000000000000 R15: ffffa0a9bfb37905 FS: 0000000000000000(0000) GS:ffffa0a9bfb00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055a45ed814e8 CR3: 000000109038a000 CR4: 0000000000350ee0 Call Trace: <TASK> ? show_trace_log_lvl+0x1d6/0x2f9 ? show_trace_log_lvl+0x1d6/0x2f9 ? mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] ? down_read+0x75/0x94 ? __warn+0x80/0x113 ? down_read+0x75/0x94 ? report_bug+0xa4/0x11d ? handle_bug+0x35/0x8b ? exc_invalid_op+0x14/0x75 ? asm_exc_invalid_op+0x16/0x1b ? down_read+0x75/0x94 ? down_read+0xe/0x94 mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] mlx5_ipsec_fs_roce_tx_destroy+0xb1/0x130 [mlx5_core] tx_destroy+0x1b/0xc0 [mlx5_core] tx_ft_put+0x53/0xc0 [mlx5_core] mlx5e_xfrm_free_state+0x45/0x90 [mlx5_core] ___xfrm_state_destroy+0x10f/0x1a2 xfrm_state_gc_task+0x81/0xa9 process_one_work+0x1f1/0x3c6 worker_thread+0x53/0x3e4 ? process_one_work.cold+0x46/0x3c kthread+0x127/0x144 ? set_kthread_struct+0x60/0x52 ret_from_fork+0x22/0x2d </TASK> ---[end trace 5ef7896144d398e1]---			
CVE-2024-45018	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload.	2024-09-11	5.5	Medium
CVE-2024-45019	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Take state lock during tx timeout reporter mlx5e_safe_reopen_channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling mlx5e_safe_reopen_channels()) to avoid the deadlock referenced in the Fixes tag.	2024-09-11	5.5	Medium
CVE-2024-45020	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a kernel verifier crash in stacksafe() Daniel Hodges reported a kernel verifier crash when playing with sched-ext. Further investigation shows that the crash is due to invalid memory access in stacksafe(). More specifically, it is the following code: if (exact != NOT_EXACT && old->stack[spi].slot_type[i % BPF_REG_SIZE] != cur->stack[spi].slot_type[i % BPF_REG_SIZE]) return false; The 'i' iterates old->allocated_stack. If cur->allocated_stack < old->allocated_stack the out-of-bound access will happen. To fix the issue add 'i >= cur->allocated_stack' check such that if the condition is true, stacksafe() should fail. Otherwise, cur->stack[spi].slot_type[i % BPF_REG_SIZE] memory access is legal.	2024-09-11	5.5	Medium
CVE-2024-45021	Linux	In the Linux kernel, the following vulnerability has been resolved:	2024-09-11	5.5	Medium

		memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane).			
CVE-2024-45022	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift. However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes __GFP_NOFAIL with high order in vm_area_alloc_pages() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE): kvmalloc(2M, __GFP_NOFAIL|GFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation failed and fallback to order-0 vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code.	2024-09-11	5.5	Medium
CVE-2024-45024	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb vs. core-mm PT locking We recently made GUP's common page table walking code to also walk hugetlb VMAs without most hugetlb special-casing, preparing for the future of having less hugetlb-specific page table walking code in the codebase. Turns out that we missed one page table locking detail: page table locking for hugetlb folios that are not mapped using a single PMD/PUD. Assume we have hugetlb folio that spans multiple PTEs (e.g., 64 KiB hugetlb folios on arm64 with 4 KiB base page size). GUP, as it walks the page tables, will perform a pte_offset_map_lock() to grab the PTE table lock. However, hugetlb that concurrently modifies these page tables would actually grab the mm->page_table_lock: with USE_SPLIT_PTE_PTLOCKS, the locks would differ. Something similar can happen right now with hugetlb folios that span multiple PMDs when USE_SPLIT_PMD_PTLOCKS. This issue can be reproduced [1], for example triggering: [3105.936100] ------------[cut here]------------ [3105.939323] WARNING: CPU: 31 PID: 2732 at mm/gup.c:142	2024-09-11	5.5	Medium

		try_grab_folio+0x11c/0x188 [3105.944634] Modules linked in: [...] [3105.974841] CPU: 31 PID: 2732 Comm: reproducer Not tainted 6.10.0-64.eln141.aarch64 #1 [3105.980406] Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-4.fc40 05/24/2024 [3105.986185] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3105.991108] pc : try_grab_folio+0x11c/0x188 [3105.994013] lr : follow_page_pte+0xd8/0x430 [3105.996986] sp : ffff80008eafb8f0 [3105.999346] x29: ffff80008eafb900 x28: ffffffe8d481f380 x27: 00f80001207cff43 [3106.004414] x26: 0000000000000001 x25: 0000000000000000 x24: ffff80008eafba48 [3106.009520] x23: 0000ffff9372f000 x22: ffff7a54459e2000 x21: ffff7a546c1aa978 [3106.014529] x20: ffffffe8d481f3c0 x19: 0000000000610041 x18: 0000000000000001 [3106.019506] x17: 0000000000000001 x16: ffffffffffffffff x15: 0000000000000000 [3106.024494] x14: ffffb85477fdfe08 x13: 0000ffff9372ffff x12: 0000000000000000 [3106.029469] x11: 1fffef4a88a96be1 x10: ffff7a54454b5f0c x9 : ffffb854771b12f0 [3106.034324] x8 : 0008000000000000 x7 : ffff7a546c1aa980 x6 : 0008000000000080 [3106.038902] x5 : 00000000001207cf x4 : 0000ffff9372f000 x3 : ffffffe8d481f000 [3106.043420] x2 : 0000000000610041 x1 : 0000000000000001 x0 : 0000000000000000 [3106.047957] Call trace: [3106.049522] try_grab_folio+0x11c/0x188 [3106.051996] follow_pmd_mask.constprop.0.isra.0+0x150/0x2e0 [3106.055527] follow_page_mask+0x1a0/0x2b8 [3106.058118] __get_user_pages+0xf0/0x348 [3106.060647] faultin_page_range+0xb0/0x360 [3106.063651] do_madvise+0x340/0x598 Let's make huge_pte_lockptr() effectively use the same PT locks as any core-mm page table walker would. Add ptep_lockptr() to obtain the PTE page table lock using a pte pointer -- unfortunately we cannot convert pte_lockptr() because virt_to_page() doesn't work with kmap'ed page tables we can have with CONFIG_HIGHPTE. Handle CONFIG_PGTABLE_LEVELS correctly by checking in reverse order, such that when e.g., CONFIG_PGTABLE_LEVELS==2 with PGDIR_SIZE==P4D_SIZE==PUD_SIZE==PMD_SIZE will work as expected. Document why that works. There is one ugly case: powerpc 8xx, whereby we have an 8 MiB hugetlb folio being mapped using two PTE page tables. While hugetlb wants to take the PMD table lock, core-mm would grab the PTE table lock of one of both PTE page tables. In such corner cases, we have to make sure that both locks match, which is (fortunately!) currently guaranteed for 8xx as it does not support SMP and consequently doesn't use split PT locks. [1] https://lore.kernel.org/all/1bbfcc7f-f222-45a5-ac44-c5a1381c596d@redhat.com/			
CVE-2024-45025	Linux	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest.	2024-09-11	5.5	Medium

		That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c			
CVE-2024-45027	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Check for xhci->interrupters being allocated in xhci_mem_clearup() If xhci_mem_init() fails, it calls into xhci_mem_cleanup() to mop up the damage. If it fails early enough, before xhci->interrupters is allocated but after xhci->max_interrupters has been set, which happens in most (all?) cases, things get uglier, as xhci_mem_cleanup() unconditionally derefences xhci->interrupters. With prejudice. Gate the interrupt freeing loop with a check on xhci->interrupters being non-NULL. Found while debugging a DMA allocation issue that led the XHCI driver on this exact path.	2024-09-11	5.5	Medium
CVE-2024-45028	Linux	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success.	2024-09-11	5.5	Medium
CVE-2024-45029	Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe On ACPI machines, the tegra i2c module encounters an issue due	2024-09-11	5.5	Medium

		to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common mutex_lock_nested acpi_subsys_runtime_resume rpm_resume tegra_i2c_xfer The problem arises because during __pm_runtime_resume(), the spinlock &dev->power.lock is acquired before rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtime_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtime_resume() on mutexes.			
CVE-2024-45030	Linux	In the Linux kernel, the following vulnerability has been resolved: igb: cope with large MAX_SKB_FRAGS Sabrina reports that the igb driver does not cope well with large MAX_SKB_FRAG values: setting MAX_SKB_FRAG to 45 causes payload corruption on TX. An easy reproducer is to run ssh to connect to the machine. With MAX_SKB_FRAGS=17 it works, with MAX_SKB_FRAGS=45 it fails. This has been reported originally in https://bugzilla.redhat.com/show_bug.cgi?id=2265320 The root cause of the issue is that the driver does not take into account properly the (possibly large) shared info size when selecting the ring layout, and will try to fit two packets inside the same 4K page even when the 1st fraglist will trump over the 2nd head. Address the issue by checking if 2K buffers are insufficient.	2024-09-11	5.5	Medium
CVE-2024-46672	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Handle SSID based pmksa deletion wpa_supplicant 2.11 sends since 1efdba5fdc2c ("Handle PMKSA flush in the driver for SAE/OWE offload cases") SSID based PMKSA del commands. brcmfmac is not prepared and tries to dereference the NULL bssid and pmkid pointers in cfg80211_pmksa. PMKID_V3 operations support SSID based updates so copy the SSID.	2024-09-11	5.5	Medium
CVE-2024-20343	Cisco	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to read any file in the file system of the underlying Linux operating system. The attacker must have valid credentials on the affected device. This vulnerability is due to incorrect validation of the arguments that are passed to a specific CLI command. An attacker could exploit this vulnerability by logging in to an affected device with low-privileged credentials and using the affected command. A successful exploit could allow the attacker access files in read-only mode on the Linux file system.	2024-09-11	5.5	Medium
CVE-2024-46677	Linux	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference	2024-09-13	5.5	Medium

		When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.)			
CVE-2024-46682	Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: prevent panic for nfsv4.0 closed files in nfs4_show_open Prior to commit 3f29cc82a84c ("nfsd: split sc_status out of sc_type") states_show() relied on sc_type field to be of valid type before calling into a subfunction to show content of a particular stateid. From that commit, we split the validity of the stateid into sc_status and no longer changed sc_type to 0 while unhashing the stateid. This resulted in kernel oopsing for nfsv4.0 opens that stay around and in nfs4_show_open() would derefence sc_file which was NULL. Instead, for closed open stateids forgo displaying information that relies of having a valid sc_file. To reproduce: mount the server with 4.0, read and close a file and then on the server cat /proc/fs/nfsd/clients/2/states [513.590804] Call trace: [513.590925] _raw_spin_lock+0xcc/0x160 [513.591119] nfs4_show_open+0x78/0x2c0 [nfsd] [513.591412] states_show+0x44c/0x488 [nfsd] [513.591681] seq_read_iter+0x5d8/0x760 [513.591896] seq_read+0x188/0x208 [513.592075] vfs_read+0x148/0x470 [513.592241] ksys_read+0xcc/0x178	2024-09-13	5.5	Medium
CVE-2024-46685	Linux	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review.	2024-09-13	5.5	Medium
CVE-2024-46686	Linux	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold.	2024-09-13	5.5	Medium
CVE-2024-46691	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Move unregister out of atomic section Commit '9329933699b3 ("soc: qcom: pmic_glink: Make client-lock non-sleeping")' moved the pmic_glink client list under a spinlock, as it is accessed by the rpmsg/glink callback, which in turn is invoked from IRQ context. This means that ucsi_unregister() is now called from atomic context, which isn't feasible as it's expecting a sleepable context. An effort is under way to get GLINK to invoke its callbacks in a sleepable context, but until then lets schedule the unregistration. A side effect of this is that ucsi_unregister() can now happen after the remote processor, and thereby the communication link with it, is gone. pmic_glink_send() is amended with a check to avoid the resulting NULL pointer dereference. This does however result in the user being informed about this	2024-09-13	5.5	Medium

		error by the following entry in the kernel log: ucsi_glink.pmic_glink_ucsi pmic_glink.ucsi.0: failed to send UCSI write request: -5			
CVE-2024-46692	Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: Mark get_wq_ctx() as atomic call Currently get_wq_ctx() is wrongly configured as a standard call. When two SMC calls are in sleep and one SMC wakes up, it calls get_wq_ctx() to resume the corresponding sleeping thread. But if get_wq_ctx() is interrupted, goes to sleep and another SMC call is waiting to be allocated a waitq context, it leads to a deadlock. To avoid this get_wq_ctx() must be an atomic call and can't be a standard SMC call. Hence mark get_wq_ctx() as a fast call.	2024-09-13	5.5	Medium
CVE-2024-46698	Linux	In the Linux kernel, the following vulnerability has been resolved: video/aperture: optionally match the device in sysfb_disable() In aperture_remove_conflicting_pci_devices(), we currently only call sysfb_disable() on vga class devices. This leads to the following problem when the pimary device is not VGA compatible: 1. A PCI device with a non-VGA class is the boot display 2. That device is probed first and it is not a VGA device so sysfb_disable() is not called, but the device resources are freed by aperture_detach_platform_device() 3. Non-primary GPU has a VGA class and it ends up calling sysfb_disable() 4. NULL pointer dereference via sysfb_disable() since the resources have already been freed by aperture_detach_platform_device() when it was called by the other device. Fix this by passing a device pointer to sysfb_disable() and checking the device to determine if we should execute it or not. v2: Fix build when CONFIG_SCREEN_INFO is not set v3: Move device check into the mutex Drop primary variable in aperture_remove_conflicting_pci_devices() Drop __init on pci sysfb_pci_dev_is_enabled()	2024-09-13	5.5	Medium
CVE-2024-41870	Adobe	Media Encoder versions 24.5, 23.6.8 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.	2024-09-13	5.5	Medium
CVE-2024-41872	Adobe	Media Encoder versions 24.5, 23.6.8 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.	2024-09-13	5.5	Medium
CVE-2024-41873	Adobe	Media Encoder versions 24.5, 23.6.8 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.	2024-09-13	5.5	Medium
CVE-2024-39382	Adobe	After Effects versions 23.6.6, 24.5 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.	2024-09-13	5.5	Medium
CVE-2024-39385	Adobe	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-09-13	5.5	Medium
CVE-2024-41867	Adobe	After Effects versions 23.6.6, 24.5 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.	2024-09-13	5.5	Medium
CVE-2024-43759	Adobe	Illustrator versions 28.6, 27.9.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application	2024-09-13	5.5	Medium

		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.			
CVE-2024-45111	Adobe	Illustrator versions 28.6, 27.9.5 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.	2024-09-13	5.5	Medium
CVE-2024-38217	Microsoft	Windows Mark of the Web Security Feature Bypass Vulnerability	2024-09-10	5.4	Medium
CVE-2024-43476	Microsoft	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-09-10	5.4	Medium
CVE-2024-7890	Citrix	Local privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	2024-09-11	5.4	Medium
CVE-2024-42424	Dell	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-09-10	5.3	Medium
CVE-2024-32006	Siemens	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application does not expire the user session on reboot without logout. This could allow an attacker to bypass Multi-Factor Authentication.	2024-09-10	5.3	Medium
CVE-2024-37994	Siemens	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected application contains a hidden configuration item to enable debug functionality. This could allow an attacker to gain insight into the internal configuration of the deployment.	2024-09-10	5.3	Medium
CVE-2024-42345	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP2). The affected application does not properly handle user session establishment and invalidation. This could allow a remote attacker to circumvent the additional multi factor authentication for user session establishment.	2024-09-10	5.3	Medium
CVE-2024-8320	Ivanti	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to spoof Network Isolation status of managed devices.	2024-09-10	5.3	Medium
CVE-2024-20390	Cisco	A vulnerability in the Dedicated XML Agent feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) on XML TCP listen port 38751. This vulnerability is due to a lack of proper error validation of ingress XML packets. An attacker could exploit this vulnerability by sending a sustained, crafted stream of XML traffic to a targeted device. A successful exploit could allow the attacker to cause XML TCP port 38751 to become unreachable while the attack traffic persists.	2024-09-11	5.3	Medium
CVE-2023-44254	Fortinet	An authorization bypass through user-controlled key [CWE-639] vulnerability in FortiAnalyzer version 7.4.1 and before 7.2.5 and FortiManager version 7.4.1 and before 7.2.5 may allow a remote	2024-09-10	5	Medium

		attacker with low privileges to read sensitive data via a crafted HTTP request.			
CVE-2024-45383	Microsoft	A mishandling of IRP requests vulnerability exists in the HDAudBus_DMA interface of Microsoft High Definition Audio Bus Driver 10.0.19041.3636 (WinBuild.160101.0800). A specially crafted application can issue multiple IRP Complete requests which leads to a local denial-of-service. An attacker can execute malicious script/application to trigger this vulnerability.	2024-09-12	5	Medium
CVE-2024-42344	Siemens	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application inserts sensitive information into a log file which is readable by all legitimate users of the underlying system. This could allow an authenticated attacker to compromise the confidentiality of other users' configuration data.	2024-09-10	4.8	Medium
CVE-2022-45856	Fortinet	An improper certificate validation vulnerability [CWE-295] in FortiClientWindows 6.4 all versions, 7.0.0 through 7.0.7, FortiClientMac 6.4 all versions, 7.0 all versions, 7.2.0 through 7.2.4, FortiClientLinux 6.4 all versions, 7.0 all versions, 7.2.0 through 7.2.4, FortiClientAndroid 6.4 all versions, 7.0 all versions, 7.2.0 and FortiClientiOS 5.6 all versions, 6.0.0 through 6.0.1, 7.0.0 through 7.0.6 SAML SSO feature may allow an unauthenticated attacker to man-in-the-middle the communication between the FortiClient and both the service provider and the identity provider.	2024-09-10	4.8	Medium
CVE-2024-46693	Linux	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink: Fix race during initialization As pointed out by Stephen Boyd it is possible that during initialization of the pmic_glink child drivers, the protection-domain notifiers fires, and the associated work is scheduled, before the client registration returns and as a result the local "client" pointer has been initialized. The outcome of this is a NULL pointer dereference as the "client" pointer is blindly dereferenced. Timeline provided by Stephen: CPU0 CPU1 ---- ---- ucsi->client = NULL; devm_pmic_glink_register_client() client->pdr_notify(client->priv, pg->client_state) pmic_glink_ucsi_pdr_notify() schedule_work(&ucsi->register_work) <schedule away> pmic_glink_ucsi_register() ucsi_register() pmic_glink_ucsi_read_version() pmic_glink_ucsi_read() pmic_glink_ucsi_read() pmic_glink_send(ucsi->client) <client is NULL BAD> ucsi->client = client // Too late! This code is identical across the altmode, battery manager and usci child drivers. Resolve this by splitting the allocation of the "client" object and the registration thereof into two operations. This only happens if the protection domain registry is populated at the time of registration, which by the introduction of commit '1ebcde047c54 ("soc: qcom: add pd-mapper implementation")' became much more likely.	2024-09-13	4.7	Medium
CVE-2024-39574	Dell	Dell PowerScale InsightIQ, version 5.1, contain an Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	2024-09-10	4.4	Medium
CVE-2024-39582	Dell	Dell PowerScale InsightIQ, version 5.0, contain a Use of hard coded Credentials vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-09-10	4.4	Medium
CVE-2024-44096	Google	there is a possible arbitrary read due to an insecure default value. This could lead to local information disclosure with System	2024-09-13	4.4	Medium

		execution privileges needed. User interaction is not needed for exploitation.			
CVE-2024-8372	Google	Improper sanitization of the value of the '[srcset]' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing . This issue affects AngularJS versions 1.3.0-rc.4 and greater. Note: The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .	2024-09-09	4.3	Medium
CVE-2024-8373	Google	Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing . This issue affects all versions of AngularJS. Note: The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .	2024-09-09	4.3	Medium
CVE-2024-27257	IBM	IBM OpenPages 8.3 and 9.0 potentially exposes information about client-side source code through use of JavaScript source maps to unauthorized users.	2024-09-10	4.3	Medium
CVE-2024-31490	Fortinet	An exposure of sensitive information to an unauthorized actor in Fortinet FortiSandbox version 4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.5 and 3.2.2 through 3.2.4 and 3.1.5 allows attacker to information disclosure via HTTP get requests.	2024-09-10	4.3	Medium
CVE-2024-45323	Fortinet	An improper access control vulnerability [CWE-284] in FortiEDR Manager API 6.2.0 through 6.2.2, 6.0 all versions may allow in a shared environment context an authenticated admin with REST API permissions in his profile and restricted to a specific organization to access backend logs that include information related to other organizations.	2024-09-10	4.3	Medium
CVE-2024-43180	IBM	IBM Concert 1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2024-09-13	4.3	Medium
CVE-2024-45103	Lenovo	A valid, authenticated LXCA user may be able to unmanage an LXCA managed device in through the LXCA web interface without sufficient privileges.	2024-09-13	4.3	Medium
CVE-2024-8059	Lenovo	IPMI credentials may be captured in XCC audit log entries when the account username length is 16 characters.	2024-09-13	4.3	Medium
CVE-2024-35282	Fortinet	A cleartext storage of sensitive information in memory vulnerability [CWE-316] affecting FortiClient VPN iOS 7.2 all versions, 7.0 all versions, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an unauthenticated attacker that has physical access to a jailbroken device to obtain cleartext passwords via keychain dump.	2024-09-10	4.2	Medium
CVE-2024-36511	Fortinet	An improperly implemented security check for standard vulnerability [CWE-358] in FortiADC Web Application Firewall (WAF) 7.4.0 through 7.4.4, 7.2 all versions, 7.1 all versions, 7.0 all versions, 6.2 all versions, 6.1 all versions, 6.0 all versions when cookie security policy is enabled may allow an attacker, under specific conditions, to retrieve the initial encrypted and signed cookie protected by the feature	2024-09-10	3.7	Low
CVE-2024-37995	Siemens	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-	2024-09-10	2.1	Low

		0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected application improperly handles error while a faulty certificate upload leading to crashing of application. This vulnerability could allow an attacker to disclose sensitive information.			

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

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