الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

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 7th of April to 13th of April. 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**

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

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 ٧ ابريل إلى١٣ ابريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-45590	Fortinet	An improper control of generation of code ('code injection') in Fortinet FortiClientLinux version 7.2.0, 7.0.6 through 7.0.10 and 7.0.3 through 7.0.4 allows attacker to execute unauthorized code or commands via tricking a FortiClientLinux user into visiting a malicious website	2024-04-09	9.6	Critical
CVE-2023-6318	LG	A command injection vulnerability exists in the processAnalyticsReport method from the com.webos.service.cloudupload service on webOS version 5 through 7. A series of specially crafted requests can lead to command execution as the root user. An attacker can make authenticated requests to trigger this vulnerability. Full versions and TV models affected: * webOS 5.5.0 - 04.50.51 running on OLED55CXPUA * webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50 running on OLED48C1PUB * webOS 7.3.1-43 (mullet-mebin) - 03.33.85 running on OLED55A23LA	2024-04-09	9.1	Critical
CVE-2023-6319	LG	A command injection vulnerability exists in the getAudioMetadata method from the com.webos.service.attachedstoragemanager service on webOS version 4 through 7. A series of specially crafted requests can lead to command execution as the root user. An attacker can make authenticated requests to trigger this vulnerability. * webOS 4.9.7 - 5.30.40 running on LG43UM7000PLA * webOS 5.5.0 - 04.50.51 running on OLED55CXPUA * webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50 running on OLED48C1PUB * webOS 7.3.1-43 (mullet-mebin) - 03.33.85 running on OLED55A23LA	2024-04-09	9.1	Critical
CVE-2023-6320	LG	A command injection vulnerability exists in the com.webos.service.connectionmanager/tv/setVlanStaticAddress endpoint on webOS versions 5 and 6. A series of specially crafted requests can lead to command execution as the dbus user. An attacker can make authenticated requests to trigger this vulnerability. Full versions and TV models affected: * webOS 5.5.0 - 04.50.51 running on OLED55CXPUA * webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50 running on OLED48C1PUB	2024-04-09	9.1	Critical

CVE-2024-29990	Microsoft	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	2024-04-09	9	Critical
CVE-2024-20758	Adobe	Adobe Commerce versions 2.4.6-p4, 2.4.5-p6, 2.4.4-p7, 2.4.7-beta3 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but the attack complexity is high.	2024-04-10	9	Critical
CVE-2024-21755	Fortinet	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSandbox version 4.4.0 through 4.4.3 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.4 allows attacker to execute unauthorized code or commands via crafted requests..	2024-04-09	8.8	High
CVE-2024-21756	Fortinet	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSandbox version 4.4.0 through 4.4.3 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.4 allows attacker to execute unauthorized code or commands via crafted requests..	2024-04-09	8.8	High
CVE-2024-20678	Microsoft	Remote Procedure Call Runtime Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-21323	Microsoft	Microsoft Defender for IoT Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26179	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26200	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26205	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26210	Microsoft	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26214	Microsoft	Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-26244	Microsoft	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28906	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28908	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28909	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28910	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28911	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28912	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28913	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28914	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28915	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28926	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28927	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28929	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28930	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28931	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28932	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28933	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28934	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28935	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28936	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28937	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28938	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28939	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28940	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High

CVE-2024-28941	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28942	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28943	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28944	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-28945	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29043	Microsoft	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29044	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29046	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29047	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29048	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29053	Microsoft	Microsoft Defender for IoT Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29982	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29983	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29984	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29985	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	8.8	High
CVE-2024-29988	Microsoft	SmartScreen Prompt Security Feature Bypass Vulnerability	2024-04-09	8.8	High
CVE-2024-29993	Microsoft	Azure CycleCloud Elevation of Privilege Vulnerability	2024-04-09	8.8	High
CVE-2024-30191	Siemens	A vulnerability has been identified in SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0), SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0), SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0), SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0), SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0), SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0), SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0), SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0), SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6), SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0), SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0), SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0), SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0), SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6), SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0), SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0), SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0), SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0), SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0), SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0), SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0), SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0), SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0), SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0), SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0), SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0), SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0), SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0), SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0), SCALANCE	2024-04-09	8.4	High

		WAM766-1 EEC (US) (6GK5766-1GE00-7TB0), SCALANCE WUM763-1 (6GK5763-1AL00-3AA0), SCALANCE WUM763-1 (6GK5763-1AL00-3DA0), SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0), SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0). This CVE refers to Scenario 3 "Override client's security context" of CVE-2022-47522. Affected devices can be tricked into associating a newly negotiated, attacker-controlled, security context with frames belonging to a victim. This could allow a physically proximate attacker to decrypt frames meant for the victim.			
CVE-2024-29050	Microsoft	Windows Cryptographic Services Remote Code Execution Vulnerability	2024-04-09	8.4	High
CVE-2024-29989	Microsoft	Azure Monitor Agent Elevation of Privilege Vulnerability	2024-04-09	8.4	High
CVE-2024-31492	Fortinet	An external control of file name or path vulnerability [CWE-73] in FortiClientMac version 7.2.3 and below, version 7.0.10 and below installer may allow a local attacker to execute arbitrary code or commands via writing a malicious configuration file in /tmp before starting the installation process.	2024-04-10	8.2	High
CVE-2023-49133	Tp-Link	A command execution vulnerability exists in the tddpd enable_test_mode functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926 and Tp-Link N300 Wireless Access Point (EAP115 V4) v5.0.4 Build 20220216. A specially crafted series of network requests can lead to arbitrary command execution. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.This vulnerability impacts \`uclited\` on the EAP225(V3) 5.1.0 Build 20220926 of the AC1350 Wireless MU-MIMO Gigabit Access Point.	2024-04-09	8.1	High
CVE-2023-49134	Tp-Link	A command execution vulnerability exists in the tddpd enable_test_mode functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926 and Tp-Link N300 Wireless Access Point (EAP115 V4) v5.0.4 Build 20220216. A specially crafted series of network requests can lead to arbitrary command execution. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.This vulnerability impacts \`uclited\` on the EAP115(V4) 5.0.4 Build 20220216 of the N300 Wireless Gigabit Access Point.	2024-04-09	8.1	High
CVE-2024-23671	Fortinet	A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiSandbox version 4.4.0 through 4.4.3 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.4 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2024-04-09	8.1	High
CVE-2024-20670	Microsoft	Outlook for Windows Spoofing Vulnerability	2024-04-09	8.1	High
CVE-2024-20759	Adobe	Adobe Commerce versions 2.4.6-p4, 2.4.5-p6, 2.4.4-p7, 2.4.7-beta3 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality and integrity are considered high due to having admin impact.	2024-04-10	8.1	High
CVE-2024-26180	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	8	High
CVE-2024-26189	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	8	High
CVE-2024-26240	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	8	High
CVE-2024-28925	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	8	High
CVE-2024-26275	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.254), Parasolid V36.0 (All versions < V36.0.207), Parasolid V36.1 (All versions < V36.1.147). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2024-04-09	7.8	High
CVE-2024-20693	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-21447	Microsoft	Windows Authentication Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26158	Microsoft	Microsoft Install Service Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26175	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.8	High
CVE-2024-26211	Microsoft	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26218	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26228	Microsoft	Windows Cryptographic Services Security Feature Bypass Vulnerability	2024-04-09	7.8	High
CVE-2024-26229	Microsoft	Windows CSC Service Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26230	Microsoft	Windows Telephony Server Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26235	Microsoft	Windows Update Stack Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26237	Microsoft	Windows Defender Credential Guard Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26239	Microsoft	Windows Telephony Server Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26241	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26245	Microsoft	Windows SMB Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-26256	Microsoft	libarchive Remote Code Execution Vulnerability	2024-04-09	7.8	High
CVE-2024-26257	Microsoft	Microsoft Excel Remote Code Execution Vulnerability	2024-04-09	7.8	High

CVE-2024-28904	Microsoft	Microsoft Brokering File System Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-28905	Microsoft	Microsoft Brokering File System Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-28907	Microsoft	Microsoft Brokering File System Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-28920	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.8	High
CVE-2024-29052	Microsoft	Windows Storage Elevation of Privilege Vulnerability	2024-04-09	7.8	High
CVE-2024-29061	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.8	High
CVE-2024-20772	Adobe	Media Encoder versions 24.2.1, 23.6.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-10	7.8	High
CVE-2021-47194	Linux	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt.	2024-04-10	7.8	High
CVE-2021-47198	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix use-after-free in lpfc_unreg_rpi() routine An error is detected with the following report when unloading the driver: "KASAN: use-after-free in lpfc_unreg_rpi+0x1b1b" The NLP_REG_LOGIN_SEND nlp_flag is set in lpfc_reg_fab_ctrl_node(), but the flag is not cleared upon completion of the login. This allows a second call to lpfc_unreg_rpi() to proceed with nlp_rpi set to LPFC_RPI_ALLOW_ERROR. This results in a use after free access when used as an rpi_ids array index. Fix by clearing the NLP_REG_LOGIN_SEND nlp_flag in lpfc_mbx_cmpl_fc_reg_login().	2024-04-10	7.8	High
CVE-2024-20795	Adobe	Animate versions 23.0.4, 24.0.1 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.	2024-04-11	7.8	High
CVE-2024-20797	Adobe	Animate versions 23.0.4, 24.0.1 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	7.8	High
CVE-2024-30271	Adobe	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	7.8	High
CVE-2024-30272	Adobe	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	7.8	High
CVE-2024-30273	Adobe	Illustrator versions 28.3, 27.9.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	7.8	High
CVE-2024-31978	Siemens	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP2). Affected devices allow authenticated users to export monitoring data. The corresponding API endpoint is susceptible to path traversal and could allow an authenticated attacker to download files from the file system. Under certain circumstances the downloaded files are deleted from the file system.	2024-04-09	7.6	High
CVE-2023-41677	Fortinet	A insufficiently protected credentials in Fortinet FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.0	2024-04-09	7.5	High

		through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17 allows attacker to execute unauthorized code or commands via targeted social engineering attack			
CVE-2023-48724	Tp-Link	A memory corruption vulnerability exists in the web interface functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted HTTP POST request can lead to denial of service of the device's web interface. An attacker can send an unauthenticated HTTP POST request to trigger this vulnerability.	2024-04-09	7.5	High
CVE-2024-26212	Microsoft	DHCP Server Service Denial of Service Vulnerability	2024-04-09	7.5	High
CVE-2024-26215	Microsoft	DHCP Server Service Denial of Service Vulnerability	2024-04-09	7.5	High
CVE-2024-26219	Microsoft	HTTP.sys Denial of Service Vulnerability	2024-04-09	7.5	High
CVE-2024-26248	Microsoft	Windows Kerberos Elevation of Privilege Vulnerability	2024-04-09	7.5	High
CVE-2024-26254	Microsoft	Microsoft Virtual Machine Bus (VMBus) Denial of Service Vulnerability	2024-04-09	7.5	High
CVE-2024-28896	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.5	High
CVE-2024-29045	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-04-09	7.5	High
CVE-2024-31871	IBM	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 could allow a malicious actor to conduct a man in the middle attack when deploying Python scripts due to improper certificate validation. IBM X-Force ID: 287306.	2024-04-10	7.5	High
CVE-2024-31872	IBM	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 could allow a malicious actor to conduct a man in the middle attack when deploying Open Source scripts due to missing certificate validation. IBM X-Force ID: 287316.	2024-04-10	7.5	High
CVE-2024-31873	IBM	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 contains hard-coded credentials which it uses for its own inbound authentication that could be obtained by a malicious actor. IBM X-Force ID: 287317.	2024-04-10	7.5	High
CVE-2023-49074	Tp-Link	A denial of service vulnerability exists in the TDDP functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of network requests can lead to reset to factory settings. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.	2024-04-09	7.4	High
CVE-2024-26194	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.4	High
CVE-2024-22450	Dell	Dell Alienware Command Center, versions prior to 6.2.7.0, contain an uncontrolled search path element vulnerability. A local malicious user could potentially inject malicious files in the file search path, leading to system compromise.	2024-04-10	7.4	High
CVE-2024-21409	Microsoft	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	2024-04-09	7.3	High
CVE-2024-26216	Microsoft	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	2024-04-09	7.3	High
CVE-2024-26232	Microsoft	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	2024-04-09	7.3	High
CVE-2024-29063	Microsoft	Azure AI Search Information Disclosure Vulnerability	2024-04-09	7.3	High
CVE-2023-6317	LG	A prompt bypass exists in the secondscreen.gateway service running on webOS version 4 through 7. An attacker can create a privileged account without asking the user for the security PIN. Full versions and TV models affected: webOS 4.9.7 - 5.30.40 running on LG43UM7000PLA webOS 5.5.0 - 04.50.51 running on OLED55CXPUA webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50 running on OLED48C1PUB webOS 7.3.1-43 (mullet-mebin) - 03.33.85 running on OLED55A23LA	2024-04-09	7.2	High
CVE-2023-49906	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `ssid` parameter at offset `0x0045ab7c` of the `httpd_portal` binary shipped with v5.1.0 Build 20220926 of the EAP225.	2024-04-09	7.2	High
CVE-2023-49907	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `band` parameter at offset `0x0045aad8` of the `httpd_portal` binary shipped with v5.1.0 Build 20220926 of the EAP225.	2024-04-09	7.2	High
CVE-2023-49908	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350	2024-04-09	7.2	High

		Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `profile` parameter at offset `0x0045abc8` of the `httpd_portal` binary shipped with v5.1.0 Build 20220926 of the EAP225.			
CVE-2023-49909	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `action` parameter at offset `0x0045ab38` of the `httpd_portal` binary shipped with v5.1.0 Build 20220926 of the EAP225.	2024-04-09	7.2	High
CVE-2023-49910	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `ssid` parameter at offset `0x42247c` of the `httpd` binary shipped with v5.0.4 Build 20220216 of the EAP115.	2024-04-09	7.2	High
CVE-2023-49911	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `band` parameter at offset `0x422420` of the `httpd` binary shipped with v5.0.4 Build 20220216 of the EAP115.	2024-04-09	7.2	High
CVE-2023-49912	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `profile` parameter at offset `0x4224b0` of the `httpd` binary shipped with v5.0.4 Build 20220216 of the EAP115.	2024-04-09	7.2	High
CVE-2023-49913	Tp-Link	A stack-based buffer overflow vulnerability exists in the web interface Radio Scheduling functionality of Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.This vulnerability refers specifically to the overflow that occurs via the `action` parameter at offset `0x422448` of the `httpd` binary shipped with v5.0.4 Build 20220216 of the EAP115.	2024-04-09	7.2	High
CVE-2024-21322	Microsoft	Microsoft Defender for IoT Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-21324	Microsoft	Microsoft Defender for IoT Elevation of Privilege Vulnerability	2024-04-09	7.2	High
CVE-2024-26195	Microsoft	DHCP Server Service Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26202	Microsoft	DHCP Server Service Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26208	Microsoft	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26221	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26222	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26223	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26224	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26227	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26231	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-26233	Microsoft	Windows DNS Server Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-29054	Microsoft	Microsoft Defender for IoT Elevation of Privilege Vulnerability	2024-04-09	7.2	High
CVE-2024-29055	Microsoft	Microsoft Defender for IoT Elevation of Privilege Vulnerability	2024-04-09	7.2	High
CVE-2024-29066	Microsoft	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	2024-04-09	7.2	High
CVE-2024-20688	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.1	High
CVE-2024-20689	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.1	High
CVE-2024-29062	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	7.1	High
CVE-2024-26213	Microsoft	Microsoft Brokering File System Elevation of Privilege Vulnerability	2024-04-09	7	High
CVE-2024-26236	Microsoft	Windows Update Stack Elevation of Privilege Vulnerability	2024-04-09	7	High
CVE-2024-26242	Microsoft	Windows Telephony Server Elevation of Privilege Vulnerability	2024-04-09	7	High
CVE-2024-26243	Microsoft	Windows USB Print Driver Elevation of Privilege Vulnerability	2024-04-09	7	High
CVE-2024-26168	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.8	Medium
CVE-2024-26251	Microsoft	Microsoft SharePoint Server Spoofing Vulnerability	2024-04-09	6.8	Medium
CVE-2024-26252	Microsoft	Windows rndismp6.sys Remote Code Execution Vulnerability	2024-04-09	6.8	Medium

CVE-2024-26253	Microsoft	Windows rndismp6.sys Remote Code Execution Vulnerability	2024-04-09	6.8	Medium
CVE-2024-28897	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.8	Medium
CVE-2023-47540	Fortinet	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSandbox version 4.4.0 through 4.4.2 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.5 and 3.2.0 through 3.2.4 and 3.0.5 through 3.0.7 may allows attacker to execute unauthorized code or commands via CLI.	2024-04-09	6.7	Medium
CVE-2023-47541	Fortinet	An improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiSandbox version 4.4.0 through 4.4.2 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.5 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 and 2.5.0 through 2.5.2 and 2.4.0 through 2.4.1 and 2.3.0 through 2.3.3 and 2.2.0 through 2.2.2 and 2.1.0 through 2.1.3 and 2.0.0 through 2.0.3 allows attacker to execute unauthorized code or commands via CLI.	2024-04-09	6.7	Medium
CVE-2023-47542	Fortinet	A improper neutralization of special elements used in a template engine [CWE-1336] in FortiManager versions 7.4.1 and below, versions 7.2.4 and below, and 7.0.10 and below allows attacker to execute unauthorized code or commands via specially crafted templates.	2024-04-09	6.7	Medium
CVE-2023-48784	Fortinet	A use of externally-controlled format string vulnerability [CWE-134] in FortiOS version 7.4.1 and below, version 7.2.7 and below, 7.0 all versions, 6.4 all versions command line interface may allow a local privileged attacker with super-admin profile and CLI access to execute arbitrary code or commands via specially crafted requests.	2024-04-09	6.7	Medium
CVE-2024-20669	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-26171	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-26234	Microsoft	Proxy Driver Spoofing Vulnerability	2024-04-09	6.7	Medium
CVE-2024-26250	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-28903	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-28919	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-28921	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-28924	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.7	Medium
CVE-2024-0159	Dell	Dell Alienware Command Center, versions 5.5.52.0 and prior, contain improper access control vulnerability, leading to Denial of Service on local system.	2024-04-10	6.7	Medium
CVE-2024-21424	Microsoft	Azure Compute Gallery Elevation of Privilege Vulnerability	2024-04-09	6.5	Medium
CVE-2024-26183	Microsoft	Windows Kerberos Denial of Service Vulnerability	2024-04-09	6.5	Medium
CVE-2024-26226	Microsoft	Windows Distributed File System (DFS) Information Disclosure Vulnerability	2024-04-09	6.5	Medium
CVE-2024-26193	Microsoft	Azure Migrate Remote Code Execution Vulnerability	2024-04-09	6.4	Medium
CVE-2024-28923	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.4	Medium
CVE-2024-27261	IBM	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.2 could allow a privileged user to install a potentially dangerous tar file, which could give them access to subsequent systems where the package was installed. IBM X-Force ID: 283986.	2024-04-12	6.4	Medium
CVE-2024-28898	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	6.3	Medium
CVE-2024-22358	IBM	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 280896.	2024-04-12	6.3	Medium
CVE-2023-50821	Siemens	A vulnerability has been identified in SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC04), SIMATIC WinCC Runtime Professional V17 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 1), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 16), SIMATIC WinCC V8.0 (All versions). The affected products do not properly validate the input provided in the login dialog box. An attacker could leverage this vulnerability to cause a persistent denial of service condition.	2024-04-09	6.2	Medium
CVE-2024-28917	Microsoft	Azure Arc-enabled Kubernetes Extension Cluster-Scope Elevation of Privilege Vulnerability	2024-04-09	6.2	Medium
CVE-2024-29064	Microsoft	Windows Hyper-V Denial of Service Vulnerability	2024-04-09	6.2	Medium
CVE-2024-31874	IBM	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 uses uninitialized variables when deploying that could allow a local user to cause a denial of service. IBM X-Force ID: 287318.	2024-04-10	6.2	Medium
CVE-2024-30189	Siemens	A vulnerability has been identified in SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0) (All versions), SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0) (All versions), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0) (All versions), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0) (All versions), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0) (All versions), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0) (All versions), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6) (All versions), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0) (All versions), SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6) (All versions), SCALANCE W738-1	2024-04-09	6.1	Medium

		M12 (6GK5738-1GY00-0AA0) (All versions), SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0) (All versions), SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0) (All versions), SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0) (All versions), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0) (All versions), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0) (All versions), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0) (All versions), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0) (All versions), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0) (All versions), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0) (All versions), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0) (All versions), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6) (All versions), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0) (All versions), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0) (All versions), SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6) (All versions), SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0) (All versions), SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0) (All versions), SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0) (All versions), SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0) (All versions), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0) (All versions), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0) (All versions), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0) (All versions), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0) (All versions), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0) (All versions), SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0) (All versions), SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0) (All versions), SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0) (All versions), SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0) (All versions), SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0) (All versions), SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0) (All versions), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0) (All versions), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0) (All versions), SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0) (All versions), SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0) (All versions), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0) (All versions), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0) (All versions), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0) (All versions), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0) (All versions), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0) (All versions), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0) (All versions). This CVE refers to Scenario 1 "Leak frames from the Wi-Fi queue" of CVE-2022-47522. Affected devices queue frames in order to subsequently change the security context and leak the queued frames. This could allow a physically proximate attacker to intercept (possibly cleartext) target-destined frames.			
CVE-2024-30190	Siemens	A vulnerability has been identified in SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0), SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0), SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0), SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0), SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0), SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0), SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0), SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0), SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6), SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0), SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6), SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0), SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0), SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0), SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0), SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0), SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0), SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0), SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0), SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6), SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0), SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0), SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0), SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0), SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0), SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0), SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0), SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0),	2024-04-09	6.1	Medium

		SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0), SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0), SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0), SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0), SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0), SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0), SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0), SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0), SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0), SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0), SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0), SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0), SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0), SCALANCE WUM763-1 (6GK5763-1AL00-3AA0), SCALANCE WUM763-1 (6GK5763-1AL00-3DA0), SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0), SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0). This CVE refers to Scenario 2 "Abuse the queue for network disruptions" of CVE-2022-47522. Affected devices can be tricked into enabling its power-saving mechanisms for a victim client. This could allow a physically proximate attacker to execute disconnection and denial-of-service attacks.			
CVE-2024-20665	Microsoft	BitLocker Security Feature Bypass Vulnerability	2024-04-09	6.1	Medium
CVE-2024-22359	IBM	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 280897.	2024-04-12	6.1	Medium
CVE-2024-31487	Fortinet	A improper limitation of a pathname to a restricted directory ('path traversal') 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 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 and 2.5.0 through 2.5.2 and 2.4.0 through 2.4.1 may allows attacker to information disclosure via crafted http requests.	2024-04-09	5.9	Medium
CVE-2024-20685	Microsoft	Azure Private 5G Core Denial of Service Vulnerability	2024-04-09	5.9	Medium
CVE-2023-50949	IBM	IBM QRadar SIEM 7.5 could allow an unauthorized user to perform unauthorized actions due to improper certificate validation. IBM X-Force ID: 275706.	2024-04-11	5.9	Medium
CVE-2024-0157	Dell	Dell Storage Resource Manager, 4.9.0.0 and below, contain(s) a Session Fixation Vulnerability in SRM Windows Host Agent. An adjacent network unauthenticated attacker could potentially exploit this vulnerability, leading to the hijack of a targeted user's application session.	2024-04-12	5.9	Medium
CVE-2024-26172	Microsoft	Windows DWM Core Library Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-26207	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-26209	Microsoft	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-26217	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-26255	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-28900	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-28901	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-28902	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-29992	Microsoft	Azure Identity Library for .NET Information Disclosure Vulnerability	2024-04-09	5.5	Medium
CVE-2024-20737	Adobe	After Effects versions 24.1, 23.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-10	5.5	Medium
CVE-2024-20766	Adobe	InDesign Desktop versions 18.5.1, 19.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-10	5.5	Medium
CVE-2024-20770	Adobe	Photoshop Desktop versions 24.7.2, 25.3.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of	2024-04-10	5.5	Medium

		this issue requires user interaction in that a victim must open a malicious file.			
CVE-2021-47193	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Fix memory leak during rmmod Driver failed to release all memory allocated. This would lead to memory leak during driver removal. Properly free memory when the module is removed.	2024-04-10	5.5	Medium
CVE-2021-47195	Linux	In the Linux kernel, the following vulnerability has been resolved: spi: fix use-after-free of the add_lock mutex Commit 6098475d4cb4 ("spi: Fix deadlock when adding SPI controllers on SPI buses") introduced a per-controller mutex. But mutex_unlock() of said lock is called after the controller is already freed: spi_unregister_controller(ctlr) -> put_device(&ctlr->dev) -> spi_controller_release(dev) -> mutex_unlock(&ctrl->add_lock) Move the put_device() after the mutex_unlock().	2024-04-10	5.5	Medium
CVE-2024-20771	Adobe	Bridge versions 13.0.6, 14.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	5.5	Medium
CVE-2024-20798	Adobe	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	5.5	Medium
CVE-2024-20794	Adobe	Animate versions 23.0.4, 24.0.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service. An attacker could leverage this vulnerability to cause a system crash, resulting in a denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	5.5	Medium
CVE-2024-20796	Adobe	Animate versions 23.0.4, 24.0.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-04-11	5.5	Medium
CVE-2024-20778	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-20779	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-20780	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26046	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26047	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium

CVE-2024-26076	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26079	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26084	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26087	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26097	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26098	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2024-26122	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-10	5.4	Medium
CVE-2023-50307	IBM	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 273338.	2024-04-12	5.4	Medium
CVE-2024-22357	IBM	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 280894.	2024-04-12	5.4	Medium
CVE-2024-23662	Fortinet	An exposure of sensitive information to an unauthorized actor in Fortinet FortiOS at least version at least 7.4.0 through 7.4.1 and 7.2.0 through 7.2.5 and 7.0.0 through 7.0.15 and 6.4.0 through 6.4.15 allows attacker to information disclosure via HTTP requests.	2024-04-09	5.3	Medium
CVE-2024-26220	Microsoft	Windows Mobile Hotspot Information Disclosure Vulnerability	2024-04-09	5	Medium
CVE-2023-45186	IBM	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 268691.	2024-04-12	4.8	Medium
CVE-2023-47714	IBM	IBM Sterling File Gateway 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 271531.	2024-04-12	4.8	Medium
CVE-2024-22448	Dell	Dell BIOS contains an Out-of-Bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to denial of service.	2024-04-10	4.7	Medium
CVE-2024-22334	IBM	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 could be vulnerable to incomplete revocation of permissions when deleting a custom security resource type. When deleting a custom security type, associated	2024-04-12	4.4	Medium

		permissions of objects using that type may not be fully revoked. This could lead to incorrect reporting of permission configuration and unexpected privileges being retained. IBM X-Force ID: 279974.			
CVE-2024-29056	Microsoft	Windows Authentication Elevation of Privilege Vulnerability	2024-04-09	4.3	Medium
CVE-2024-22339	IBM	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 is vulnerable to a sensitive information due to insufficient obfuscation of sensitive values from some log files. IBM X-Force ID: 279979.	2024-04-12	4.3	Medium
CVE-2024-28922	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-04-09	4.1	Medium
CVE-2024-26276	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.254), Parasolid V36.0 (All versions < V36.0.207), Parasolid V36.1 (All versions < V36.1.147). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition.	2024-04-09	3.3	Low
CVE-2024-26277	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.254), Parasolid V36.0 (All versions < V36.0.207), Parasolid V36.1 (All versions < V36.1.147). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted X_T files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-04-09	3.3	Low

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

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