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 ٧ يوليو إلى ١٣ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 7th of July to 13th of July. 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-2024-38089	Microsoft	Microsoft Defender for IoT Elevation of Privilege Vulnerability	2024-07-09	9.9	Critical
CVE-2024-6602	Mozilla	A mismatch between allocator and deallocator could have lead to memory corruption. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	2024-07-09	9.8	Critical
CVE-2024-6606	Mozilla	Clipboard code failed to check the index on an array access. This could have lead to an out-of-bounds read. This vulnerability affects Firefox < 128 and Thunderbird < 128.	2024-07-09	9.8	Critical
CVE-2024-6611	Mozilla	A nested iframe, triggering a cross-site navigation, could send SameSite=Strict or Lax cookies. This vulnerability affects Firefox < 128 and Thunderbird < 128.	2024-07-09	9.8	Critical
CVE-2024-38074	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	Critical
CVE-2024-38076	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	Critical
CVE-2024-38077	Microsoft	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	Critical
CVE-2024-39872	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly assign rights to temporary files created during its update process. This could allow an authenticated attacker with the 'Manage firmware updates' role to escalate their privileges on the underlying OS level.	2024-07-09	9.3	Critical
CVE-2024-23663	Fortinet	An improper access control in Fortinet FortiExtender 4.1.1 - 4.1.9, 4.2.0 - 4.2.6, 5.3.2, 7.0.0 - 7.0.4, 7.2.0 - 7.2.4 and 7.4.0 - 7.4.2 allows an attacker to create users with elevated privileges via a crafted HTTP request.	2024-07-09	8.8	High
CVE-2024-27784	Fortinet	Multiple Exposure of sensitive information to an unauthorized actor vulnerabilities [CWE-200] in FortiAIOps version 2.0.0 may allow an authenticated, remote attacker to retrieve sensitive information from the API endpoint or log files.	2024-07-09	8.8	High
CVE-2024-20701	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21303	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21308	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21317	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21331	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21332	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21333	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21335	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21373	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High

CVE-2024-21398	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21414	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21415	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21425	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21428	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21449	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-28899	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8.8	High
CVE-2024-28928	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-30013	Microsoft	Windows MultiPoint Services Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-35256	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-35271	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-35272	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37318	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37319	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37320	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37321	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37322	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37323	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37324	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37326	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37327	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37328	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37329	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37330	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37331	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37332	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37333	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37334	Microsoft	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-37336	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38021	Microsoft	Microsoft Outlook Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38053	Microsoft	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38060	Microsoft	Windows Imaging Component Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38087	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38088	Microsoft	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-38092	Microsoft	Azure CycleCloud Elevation of Privilege Vulnerability	2024-07-09	8.8	High
CVE-2024-38104	Microsoft	Windows Fax Service Remote Code Execution Vulnerability	2024-07-09	8.8	High
CVE-2024-21417	Microsoft	Windows Text Services Framework Elevation of Privilege Vulnerability	2024-07-10	8.8	High
CVE-2024-39570	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input sanitation when loading VxLAN configurations. This could allow an authenticated attacker to execute arbitrary code with root privileges.	2024-07-09	8.7	High
CVE-2024-39571	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input	2024-07-09	8.7	High

		sanitation when loading SNMP configurations. This could allow an attacker with the right to modify the SNMP configuration to execute arbitrary code with root privileges.			
CVE-2024-39675	Siemens	A vulnerability has been identified in RUGGEDCOM RMC30 (All versions < V4.3.10), RUGGEDCOM RMC30NC (All versions < V4.3.10), RUGGEDCOM RP110 (All versions < V4.3.10), RUGGEDCOM RP110NC (All versions < V4.3.10), RUGGEDCOM RS400 (All versions < V4.3.10), RUGGEDCOM RS400NC (All versions < V4.3.10), RUGGEDCOM RS401 (All versions < V4.3.10), RUGGEDCOM RS401NC (All versions < V4.3.10), RUGGEDCOM RS416 (All versions < V4.3.10), RUGGEDCOM RS416NC (All versions < V4.3.10), RUGGEDCOM RS416NCv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416P (All versions < V4.3.10), RUGGEDCOM RS416PNC (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS910 (All versions < V4.3.10), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910LNC (All versions), RUGGEDCOM RS910NC (All versions < V4.3.10), RUGGEDCOM RS910W (All versions < V4.3.10), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920LNC (All versions), RUGGEDCOM RS920W (All versions). In some configurations the affected products wrongly enable the Modbus service in non-managed VLANS. Only serial devices are affected by this vulnerability.	2024-07-09	8.7	High
CVE-2024-39865	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. As part of this backup, files can be restored without correctly checking the path of the restored file. This could allow an attacker with access to the backup encryption key to upload malicious files, that could potentially lead to remote code execution.	2024-07-09	8.7	High
CVE-2024-39866	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. This could allow an attacker with access to the backup encryption key and with the right to upload backup files to create a user with administrative privileges.	2024-07-09	8.7	High
CVE-2024-39873	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its web API. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	2024-07-09	8.7	High
CVE-2024-39874	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its Client Communication component. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	2024-07-09	8.7	High
CVE-2024-39888	Siemens	A vulnerability has been identified in Mendix Encryption (All versions >= V10.0.0 < V10.0.2). Affected versions of the module define a specific hard-coded default value for the EncryptionKey constant, which is used in projects where no individual EncryptionKey was specified. This could allow to an attacker to decrypt any encrypted project data, as the default encryption key can be considered compromised.	2024-07-09	8.7	High
CVE-2024-37999	Siemens	A vulnerability has been identified in Medicalis Workflow Orchestrator (All versions). The affected application executes as a trusted account with high privileges and network access. This could allow an authenticated local attacker to escalate privileges.	2024-07-08	8.5	High
CVE-2022-45147	Siemens	A vulnerability has been identified in SIMATIC PCS neo V4.0 (All versions), SIMATIC STEP 7 V16 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	8.5	High

CVE-2024-39567	Siemens	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	2024-07-09	8.5	High
CVE-2024-39568	Siemens	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading proxy configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	2024-07-09	8.5	High
CVE-2024-6151	Citrix	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Virtual Delivery Agent for Windows used by Citrix Virtual Apps and Desktops and Citrix DaaS	2024-07-10	8.5	High
CVE-2024-6286	Citrix	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	2024-07-10	8.5	High
CVE-2024-37984	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8.4	High
CVE-2024-23695	Google	In CacheOpPMRExec of cache_km.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	High
CVE-2024-23696	Google	In RGXCreateZSBufferKM of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	High
CVE-2024-31319	Google	In updateNotificationChannelFromPrivilegedListener of NotificationManagerService.java, there is a possible cross-user data leak 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.	2024-07-09	8.4	High
CVE-2024-31332	Google	In multiple locations, there is a possible way to bypass a restriction on adding new Wi-Fi connections due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	High
CVE-2024-30321	Siemens	A vulnerability has been identified in SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 23), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 17), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5). The affected products do not properly handle certain requests to their web application, which may lead to the leak of privileged information. This could allow an unauthenticated remote attacker to retrieve information such as users and passwords.	2024-07-09	8.2	High
CVE-2024-38867	Siemens	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V9.64), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions < V9.64), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions < V9.64), SIPROTEC 5 6MD89 (CP300) (All versions < V9.64), SIPROTEC 5 6MU85 (CP300) (All versions < V9.64), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions < V9.64), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.65), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions < V9.65), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions < V9.65), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.65), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions < V9.65), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ81 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ82 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions < V9.65), SIPROTEC 5 7SK82 (CP100) (All versions < V8.89), SIPROTEC 5 7SK82 (CP150) (All versions < V9.65), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions < V9.65), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.65), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions < V9.65), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions < V9.65), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions < V9.64),	2024-07-09	8.2	High

		SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST86 (CP300) (All versions < V9.64), SIPROTEC 5 7SX82 (CP150) (All versions < V9.65), SIPROTEC 5 7SX85 (CP300) (All versions < V9.65), SIPROTEC 5 7UM85 (CP300) (All versions < V9.64), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.65), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions < V9.65), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions < V9.65), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions < V9.65), SIPROTEC 5 7VE85 (CP300) (All versions < V9.64), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions < V9.65), SIPROTEC 5 7VU85 (CP300) (All versions < V9.64), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BD-2FO (All versions < V9.62), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.64). The affected devices are supporting weak ciphers on several ports (443/tcp for web, 4443/tcp for DIGSI 5 and configurable port for syslog over TLS). This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from those ports.			
CVE-2024-39742	IBM	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 could allow a user to bypass authentication under certain configurations due to a partial string comparison vulnerability. IBM X-Force ID: 297169.	2024-07-08	8.1	High
CVE-2024-27782	Fortinet	Multiple insufficient session expiration vulnerabilities [CWE-613] in FortiAIOps version 2.0.0 may allow an attacker to re-use stolen old session tokens to perform unauthorized operations via crafted requests.	2024-07-09	8.1	High
CVE-2024-35264	Microsoft	.NET and Visual Studio Remote Code Execution Vulnerability	2024-07-09	8.1	High
CVE-2024-38049	Microsoft	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability	2024-07-09	8.1	High
CVE-2024-22280	VMware	VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product. An authenticated malicious user could enter specially crafted SQL queries and perform unauthorised read/write operations in the database.	2024-07-11	8.1	High
CVE-2024-37969	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37970	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37971	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37972	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37974	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37975	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37977	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37978	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37981	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37986	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37987	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37988	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-37989	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-38010	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-38011	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	High
CVE-2024-38330	IBM	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 295227.	2024-07-08	7.8	High
CVE-2024-4944	WatchGuard	A local privilege escalation vlnerability in the WatchGuard Mobile VPN with SSL client on Windows enables a local user to execute arbitrary commands with elevated privileged.	2024-07-09	7.8	High
CVE-2024-30079	Microsoft	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-35261	Microsoft	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-37973	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	7.8	High
CVE-2024-38034	Microsoft	Windows Filtering Platform Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38043	Microsoft	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38047	Microsoft	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38050	Microsoft	Windows Workstation Service Elevation of Privilege Vulnerability	2024-07-09	7.8	High

CVE-2024-38051	Microsoft	Windows Graphics Component Remote Code Execution Vulnerability	2024-07-09	7.8	High
CVE-2024-38052	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38054	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38057	Microsoft	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38059	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38062	Microsoft	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38066	Microsoft	Windows Win32k Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38070	Microsoft	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability	2024-07-09	7.8	High
CVE-2024-38079	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38080	Microsoft	Windows Hyper-V Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38085	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-38100	Microsoft	Windows File Explorer Elevation of Privilege Vulnerability	2024-07-09	7.8	High
CVE-2024-20781	Adobe	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-09	7.8	High
CVE-2024-20782	Adobe	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-09	7.8	High
CVE-2024-20783	Adobe	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-09	7.8	High
CVE-2024-20785	Adobe	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-09	7.8	High
CVE-2024-34139	Adobe	Bridge versions 14.0.4, 13.0.7, 14.1 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.	2024-07-09	7.8	High
CVE-2023-21113	Google	In multiple locations, there is a possible permission bypass 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.	2024-07-09	7.8	High
CVE-2024-23698	Google	In RGXFWChangeOSidPriority of rgxfwutils.c, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-23711	Google	In DevmemXIntUnreserveRange of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-31316	Google	In onResult of AccountManagerService.java, there is a possible way to perform an arbitrary background activity launch due to parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-31317	Google	In multiple functions of ZygoteProcess.java, there is a possible way to achieve code execution as any app via WRITE_SECURE_SETTINGS due to unsafe deserialization. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-31323	Google	In onCreate of multiple files, there is a possible way to trick the user into granting health permissions due to tapjacking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-31324	Google	In hide of WindowState.java, there is a possible way to bypass tapjacking/overlay protection by launching the activity in portrait mode first and then rotating it to landscape mode. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	2024-07-09	7.8	High
CVE-2024-31331	Google	In setMimeGroup of PackageManagerService.java, there is a possible way to hide the service from Settings due to a logic error in the code. This could lead to local escalation of privilege with	2024-07-09	7.8	High

		User execution privileges needed. User interaction is needed for exploitation.			
CVE-2024-31339	Google	In multiple functions of StatsService.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2024-34726	Google	In PVRSRV_MMap of pvr_bridge_k.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	High
CVE-2023-52237	Siemens	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The web server of the affected devices allow a low privileged user to access hashes and password salts of all system's users, including admin users. An attacker could use the obtained information to brute force the passwords offline.	2024-07-09	7.7	High
CVE-2024-27783	Fortinet	Multiple cross-site request forgery (CSRF) vulnerabilities [CWE-352] in FortiAIOps version 2.0.0 may allow an unauthenticated remote attacker to perform arbitrary actions on behalf of an authenticated user via tricking the victim to execute malicious GET requests.	2024-07-09	7.6	High

CVE-2024-35266	Microsoft	Azure DevOps Server Spoofing Vulnerability	2024-07-09	7.6	High
CVE-2024-35267	Microsoft	Azure DevOps Server Spoofing Vulnerability	2024-07-09	7.6	High
CVE-2024-38278	Siemens	A vulnerability has been identified in RUGGEDCOM RMC8388 V5.X (All versions < V5.9.0), RUGGEDCOM RMC8388NC V5.X (All versions < V5.9.0), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900GNC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300P V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG907R (All versions < V5.9.0), RUGGEDCOM RSG908C (All versions < V5.9.0), RUGGEDCOM RSG909R (All versions < V5.9.0), RUGGEDCOM RSG910C (All versions < V5.9.0), RUGGEDCOM RSG920P V5.X (All versions < V5.9.0), RUGGEDCOM RSG920PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSL910 (All versions < V5.9.0), RUGGEDCOM RSL910NC (All versions < V5.9.0), RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0), RUGGEDCOM RST916C (All versions < V5.9.0), RUGGEDCOM RST916P (All versions < V5.9.0). The affected products with IP forwarding enabled wrongly make available certain remote services in non-managed VLANs, even if these services are not intentionally activated. An attacker could leverage this vulnerability to create a remote shell to the affected system.	2024-07-09	7.5	High
CVE-2024-39569	Siemens	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an administrative remote attacker running a corresponding SINEMA Remote Connect Server to execute arbitrary code with system privileges on the client system.	2024-07-09	7.5	High
CVE-2024-30098	Microsoft	Windows Cryptographic Services Security Feature Bypass Vulnerability	2024-07-09	7.5	High
CVE-2024-30105	Microsoft	.NET Core and Visual Studio Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-32987	Microsoft	Microsoft SharePoint Server Information Disclosure Vulnerability	2024-07-09	7.5	High
CVE-2024-38015	Microsoft	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38031	Microsoft	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38061	Microsoft	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability	2024-07-09	7.5	High
CVE-2024-38064	Microsoft	Windows TCP/IP Information Disclosure Vulnerability	2024-07-09	7.5	High
CVE-2024-38067	Microsoft	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38068	Microsoft	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38071	Microsoft	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38072	Microsoft	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38073	Microsoft	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38078	Microsoft	Xbox Wireless Adapter Remote Code Execution Vulnerability	2024-07-09	7.5	High
CVE-2024-38091	Microsoft	Microsoft WS-Discovery Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38095	Microsoft	.NET and Visual Studio Denial of Service Vulnerability	2024-07-09	7.5	High
CVE-2024-38112	Microsoft	Windows MSHTML Platform Spoofing Vulnerability	2024-07-09	7.5	High
CVE-2024-6603	Mozilla	In an out-of-memory scenario an allocation could fail but free would have been called on the pointer afterwards leading to memory corruption. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	2024-07-09	7.4	High
CVE-2023-50178	Fortinet	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2.0 through 7.2.3, 7.1 all versions, 7.0 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and various remote servers such as private SDN connectors and FortiToken Cloud.	2024-07-09	7.4	High
CVE-2024-31320	Google	In setSkipPrompt of AssociationRequest.java , there is a possible way to establish a companion device association without any	2024-07-09	7.4	High

		confirmation due to CDM. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2024-34720	Google	In com_android_internal_os_ZygoteCommandBuffer_nativeForkRepeatedly of com_android_internal_os_ZygoteCommandBuffer.cpp, there is a possible method to perform arbitrary code execution in any app zygote processes 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.	2024-07-09	7.4	High
CVE-2024-34722	Google	In smp_proc_rand of smp_act.cc, there is a possible authentication bypass during legacy BLE pairing due to incorrect implementation of a protocol. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.4	High
CVE-2024-32056	Siemens	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS part file. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.3	High
CVE-2024-33653	Siemens	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.3	High
CVE-2024-33654	Siemens	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.3	High
CVE-2024-37997	Siemens	A vulnerability has been identified in JT Open (All versions < V11.5), PLM XML SDK (All versions < V7.1.0.014). The affected applications contain a stack based overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.3	High
CVE-2024-30061	Microsoft	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2024-07-09	7.3	High
CVE-2024-38033	Microsoft	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.3	High
CVE-2024-38081	Microsoft	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	2024-07-09	7.3	High
CVE-2024-23697	Google	In RGXCreateHWRTData_aux of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.3	High
CVE-2024-6677	Citrix	Privilege escalation in uberAgent	2024-07-12	7.3	High
CVE-2024-5974	WatchGuard	A buffer overflow in WatchGuard Fireware OS could may allow an authenticated remote attacker with privileged management access to execute arbitrary code with system privileges on the firewall. This issue affects Fireware OS: from 11.9.6 through 12.10.3.	2024-07-09	7.2	High
CVE-2024-39867	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit device configuration information of devices for which they have no privileges.	2024-07-09	7.2	High
CVE-2024-39868	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit VxLAN configuration information of networks for which they have no privileges.	2024-07-09	7.2	High
CVE-2024-38019	Microsoft	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38023	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38024	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38025	Microsoft	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38028	Microsoft	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38044	Microsoft	DHCP Server Service Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-38094	Microsoft	Microsoft SharePoint Remote Code Execution Vulnerability	2024-07-09	7.2	High
CVE-2024-35154	IBM	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote authenticated attacker, who has authorized access to the administrative console, to execute arbitrary code. Using specially crafted input, the attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 292641.	2024-07-09	7.2	High

CVE-2024-39869	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected products allow to upload certificates. An authenticated attacker could upload a crafted certificates leading to a permanent denial-of-service situation. In order to recover from such an attack, the offending certificate needs to be removed manually.	2024-07-09	7.1	High
CVE-2024-39870	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected applications can be configured to allow users to manage own users. A local authenticated user with this privilege could use this modify users outside of their own scope as well as to escalate privileges.	2024-07-09	7.1	High
CVE-2024-30081	Microsoft	Windows NTLM Spoofing Vulnerability	2024-07-09	7.1	High
CVE-2024-38032	Microsoft	Microsoft Xbox Remote Code Execution Vulnerability	2024-07-09	7.1	High
CVE-2023-32735	Siemens	A vulnerability has been identified in SIMATIC STEP 7 Safety V16 (All versions < V16 Update 7), SIMATIC STEP 7 Safety V17 (All versions < V17 Update 7), SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2), SIMATIC STEP 7 V16 (All versions < V16 Update 7), SIMATIC STEP 7 V17 (All versions < V17 Update 7), SIMATIC STEP 7 V18 (All versions < V18 Update 2), SIMATIC WinCC Unified V16 (All versions < V16 Update 7), SIMATIC WinCC Unified V17 (All versions < V17 Update 7), SIMATIC WinCC Unified V18 (All versions < V18 Update 2), SIMATIC WinCC V16 (All versions < V16.7), SIMATIC WinCC V17 (All versions < V17.7), SIMATIC WinCC V18 (All versions < V18 Update 2), SIMOCODE ES V16 (All versions < V16 Update 7), SIMOCODE ES V17 (All versions < V17 Update 7), SIMOCODE ES V18 (All versions < V18 Update 2), SIMOTION SCOUT TIA V5.4 SP1 (All versions), SIMOTION SCOUT TIA V5.4 SP3 (All versions), SIMOTION SCOUT TIA V5.5 SP1 (All versions), SINAMICS Startdrive V16 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SIRIUS Safety ES V17 (All versions < V17 Update 7), SIRIUS Safety ES V18 (All versions < V18 Update 2), SIRIUS Soft Starter ES V17 (All versions < V17 Update 7), SIRIUS Soft Starter ES V18 (All versions < V18 Update 2), Soft Starter ES V16 (All versions < V16 Update 7), TIA Portal Cloud V3.0 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing hardware configuration profiles. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	7	High
CVE-2023-32737	Siemens	A vulnerability has been identified in SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	7	High
CVE-2024-38022	Microsoft	Windows Image Acquisition Elevation of Privilege Vulnerability	2024-07-09	7	High
CVE-2024-38069	Microsoft	Windows Enroll Engine Security Feature Bypass Vulnerability	2024-07-09	7	High
CVE-2024-34123	Adobe	Premiere Pro versions 23.6.5, 24.4.1 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious file into the search path, which the application might execute instead of the legitimate file. This could occur when the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction, attack complexity is high.	2024-07-09	7	High
CVE-2024-34724	Google	In _UnrefAndMaybeDestroy of pmr.c, there is a possible arbitrary code execution 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.	2024-07-09	7	High
CVE-2024-32670	Samsung	Exposure of Sensitive Information to an Unauthorized Actor in Samsung Galaxy SmartTag2 prior to 0.20.04 allows attackes to potentially identify the tag's location by scanning the BLE adversting.	2024-07-10	7	High
CVE-2024-6646	Netgear	A vulnerability was found in Netgear WN604 up to 20240710. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /downloadFile.php of the component Web Interface. The manipulation of the argument file	2024-07-10	6.9	Medium

		with the input config leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271052. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
CVE-2024-26184	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	6.8	Medium
CVE-2024-38058	Microsoft	BitLocker Security Feature Bypass Vulnerability	2024-07-09	6.8	Medium
CVE-2024-38065	Microsoft	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	6.8	Medium
CVE-2024-38013	Microsoft	Microsoft Windows Server Backup Elevation of Privilege Vulnerability	2024-07-09	6.7	Medium
CVE-2024-31334	Google	In DevmemIntFreeDefBackingPage of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	6.7	Medium
CVE-2024-38301	Dell	Dell Alienware Command Center, version 5.7.3.0 and prior, contains an improper access control vulnerability. A low privileged attacker could potentially exploit this vulnerability, leading to denial of service on the local system and information disclosure.	2024-07-10	6.7	Medium
CVE-2024-20456	Cisco	A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device. This vulnerability is due to an error in the software build process. An attacker could exploit this vulnerability by manipulating the system’s configuration options to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass of the requirement to run Cisco signed images or alter the security properties of the running system.	2024-07-10	6.7	Medium
CVE-2024-38020	Microsoft	Microsoft Outlook Spoofing Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38027	Microsoft	Windows Line Printer Daemon Service Denial of Service Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38030	Microsoft	Windows Themes Spoofing Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38048	Microsoft	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38101	Microsoft	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38102	Microsoft	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38105	Microsoft	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	Medium
CVE-2024-38086	Microsoft	Azure Kinect SDK Remote Code Execution Vulnerability	2024-07-09	6.4	Medium
CVE-2024-31311	Google	In increment_annotation_count of stats_event.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	6.3	Medium
CVE-2024-31322	Google	In updateServicesLocked of AccessibilityManagerService.java, there is a possible way for an app to be hidden from the Setting while retaining Accessibility Service due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-07-09	6.3	Medium
CVE-2024-25023	IBM	IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 281429.	2024-07-10	6.2	Medium
CVE-2024-39743	IBM	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 IBM MQ Container Developer Edition is vulnerable to denial of service caused by incorrect memory de-allocation. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 297172.	2024-07-08	5.9	Medium
CVE-2024-38099	Microsoft	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	5.9	Medium
CVE-2024-21993	NetApp	SnapCenter versions prior to 5.0p1 are susceptible to a vulnerability which could allow an authenticated attacker to discover plaintext credentials.	2024-07-09	5.7	Medium
CVE-2023-32467	Dell	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some UEFI code, leading to arbitrary code execution or escalation of privilege.	2024-07-10	5.7	Medium

CVE-2023-32472	Dell	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	2024-07-10	5.7	Medium
CVE-2024-38017	Microsoft	Microsoft Message Queuing Information Disclosure Vulnerability	2024-07-09	5.5	Medium
CVE-2024-38041	Microsoft	Windows Kernel Information Disclosure Vulnerability	2024-07-09	5.5	Medium
CVE-2024-38055	Microsoft	Microsoft Windows Codecs Library Information Disclosure Vulnerability	2024-07-09	5.5	Medium
CVE-2024-38056	Microsoft	Microsoft Windows Codecs Library Information Disclosure Vulnerability	2024-07-09	5.5	Medium
CVE-2024-34140	Adobe	Bridge versions 14.0.4, 13.0.7, 14.1 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.	2024-07-09	5.5	Medium
CVE-2024-37528	IBM	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 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: 294293.	2024-07-08	5.4	Medium
CVE-2024-27785	Fortinet	An improper neutralization of formula elements in a CSV File vulnerability [CWE-1236] in FortiAIOps version 2.0.0 may allow a remote authenticated attacker to execute arbitrary commands on a client's workstation via poisoned CSV reports.	2024-07-09	5.4	Medium
CVE-2023-35006	IBM	IBM Security QRadar EDR 3.12 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 297165.	2024-07-10	5.4	Medium
CVE-2024-40690	IBM	IBM InfoSphere Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows an authenticated 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: 297720.	2024-07-12	5.4	Medium
CVE-2023-52891	Siemens	A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.5), SIMATIC Energy Manager PRO (All versions < V7.5), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMIT V10 (All versions), SIMIT V11 (All versions < V11.1). Unified Automation .NET based OPC UA Server SDK before 3.2.2 used in Siemens products are affected by a similar vulnerability as documented in CVE-2023-27321 for the OPC Foundation UA .NET Standard implementation. A successful attack may lead to high load situation and memory exhaustion, and may block the server.	2024-07-09	5.3	Medium
CVE-2024-39871	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly separate the rights to edit device settings and to edit settings for communication relations. This could allow an authenticated attacker with the permission to manage devices to gain access to participant groups that the attacked does not belong to.	2024-07-09	5.3	Medium
CVE-2024-39875	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows authenticated, low privilege users with the 'Manage own remote connections' permission to retrieve details about other users and group memberships.	2024-07-09	5.3	Medium
CVE-2024-39876	Siemens	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly handle log rotation. This could allow an unauthenticated remote attacker to cause a denial of service condition through resource exhaustion on the device.	2024-07-09	5.3	Medium
CVE-2024-6612	Mozilla	CSP violations generated links in the console tab of the developer tools, pointing to the violating resource. This caused a DNS prefetch which leaked that a CSP violation happened. This vulnerability affects Firefox < 128 and Thunderbird < 128.	2024-07-09	5.3	Medium
CVE-2024-35270	Microsoft	Windows iSCSI Service Denial of Service Vulnerability	2024-07-09	5.3	Medium
CVE-2024-31315	Google	In multiple functions of ManagedServices.java, there is a possible way to hide an app with notification access in the Device & app notifications settings due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-07-09	5.3	Medium
CVE-2024-31327	Google	In multiple functions of MessageQueueBase.h, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	5.3	Medium
CVE-2024-34723	Google	In onTransact of ParcelableListBinder.java , there is a possible way to steal mAllowlistToken to launch an app from background due to	2024-07-09	5.3	Medium

		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.			
CVE-2023-33859	IBM	IBM Security QRadar EDR 3.12 could disclose sensitive information due to an observable login response discrepancy. IBM X-Force ID: 257697.	2024-07-10	5.3	Medium
CVE-2023-33860	IBM	IBM Security QRadar EDR 3.12 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 257702.	2024-07-10	5.3	Medium
CVE-2024-6148	Citrix	Bypass of GACS Policy Configuration settings in Citrix Workspace app for HTML5	2024-07-10	5.3	Medium
CVE-2023-50181	Fortinet	An improper access control vulnerability [CWE-284] in Fortinet FortiADC version 7.4.0 through 7.4.1 and before 7.2.4 allows a read only authenticated attacker to perform some write actions via crafted HTTP or HTTPS requests.	2024-07-09	4.9	Medium
CVE-2024-37996	Siemens	A vulnerability has been identified in JT Open (All versions < V11.5), PLM XML SDK (All versions < V7.1.0.014). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XML files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-07-09	4.8	Medium
CVE-2023-50179	Fortinet	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2 all versions, 7.1 all versions, 7.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and public SDN connectors.	2024-07-09	4.8	Medium
CVE-2024-33509	Fortinet	An improper certificate validation vulnerability [CWE-295] in FortiWeb 7.2.0 through 7.2.1, 7.0 all versions, 6.4 all versions and 6.3 all versions may allow a remote and unauthenticated attacker in a Man-in-the-Middle position to decipher and/or tamper with the communication channel between the device and different endpoints used to fetch data for Web Application Firewall (WAF).	2024-07-09	4.8	Medium
CVE-2024-6149	Citrix	Redirection of users to a vulnerable URL in Citrix Workspace app for HTML5	2024-07-10	4.8	Medium
CVE-2024-6150	Citrix	A non-admin user can cause short-term disruption in Target VM availability in Citrix Provisioning	2024-07-10	4.8	Medium
CVE-2024-30071	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-07-09	4.7	Medium
CVE-2024-39723	IBM	IBM FlashSystem 5300 USB ports may be usable even if the port has been disabled by the administrator. A user with physical access to the system could use the USB port to cause loss of access to data. IBM X-Force ID: 295935.	2024-07-08	4.6	Medium
CVE-2024-31897	IBM	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178.	2024-07-08	4.3	Medium
CVE-2024-21759	Fortinet	An authorization bypass through user-controlled key in Fortinet FortiPortal version 7.2.0, and versions 7.0.0 through 7.0.6 allows attacker to view unauthorized resources via HTTP or HTTPS requests.	2024-07-09	4.3	Medium
CVE-2024-26015	Fortinet	An incorrect parsing of numbers with different radices vulnerability [CWE-1389] in FortiProxy version 7.4.3 and below, version 7.2.10 and below, version 7.0.17 and below and FortiOS version 7.4.3 and below, version 7.2.8 and below, version 7.0.15 and below IP address validation feature may permit an unauthenticated attacker to bypass the IP blocklist via crafted requests.	2024-07-09	3.4	Low
CVE-2023-52238	Siemens	A vulnerability has been identified in RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0). The web server of the affected systems leaks the MACSEC key in clear text to a logged in user. An attacker with the credentials of a low privileged user could retrieve the MACSEC key and access (decrypt) the ethernet frames sent by authorized recipients.	2024-07-09	2.3	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.