Posted Date: 2025/06/10

□Vulnerability Alert □ CISA Adds 9 New Exploited Vulnerabilities to KEV Catalog (2025/06/02-2025/06/08)

Subject:
 [Vulnerability Alert] CISA Adds 9 New Exploited Vulnerabilities to KEV Catalog (2025/06/02-2025/06/08)

· Content:

- Forwarded from Taiwan Computer Emergency Response Team / Coordination Center TWCERTCC-200-202506-00000003
- 1. [CVE-2021-32030] ASUS Routers Improper Authentication Vulnerability (CVSS v3.1: 9.8)
 - [Ransomware Exploitation: Unknown] Improper authentication vulnerability exists in ASUS Lyra Mini and ASUS GT-AC2900 devices, allowing unauthorized access to the management interface.
 - [Affected Platforms] Versions prior to ASUS GT-AC2900 3.0.04.386.42643 and ASUS Lyra Mini 3.0.0.4 384 46630
- 2. [CVE-2025-3935] ConnectWise ScreenConnect Improper Authentication Vulnerability (CVSS v3.1: 7.2)
 - [Ransomware Exploitation: Unknown] Improper authentication vulnerability in ConnectWise ScreenConnect. This may allow ViewState code injection attacks. If the machine key is leaked, attackers may remotely execute arbitrary code.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://www.connectwise.com/company/trust/security-bulletins/screenconnect-security-patch-2025.4
- 3. [CVE-2025-35939] Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability (CVSS v3.1: 5.3)
 - [Ransomware Exploitation: Unknown] Craft CMS has a vulnerability due to insufficient validation of mutable web parameters. Attackers can exploit this to write arbitrary content (e.g., PHP code) to a specified local file path on the server, potentially leading to remote code execution.
 - [Affected Platforms] Versions prior to Craft CMS 4.15.3 and versions from 5.00 to before 5.7.5
- 4. [CVE-2024-56145] Craft CMS Code Injection Vulnerability (CVSS v3.1: 9.8)
 - [Ransomware Exploitation: Unknown] Craft CMS has a code injection vulnerability. If users of affected versions have enabled `register_argc_argv` in their php.ini settings, they are vulnerable to remote code execution.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://github.com/craftcms/cms/security/advisories/GHSA-2p6p-9rc9-62j9
- 5. [CVE-2023-39780] ASUS RT-AX55 Routers OS Command Injection Vulnerability (CVSS v3.1: 8.8)
 - [Ransomware Exploitation: Unknown] ASUS RT-AX55 devices have an OS command injection vulnerability. Remote and authenticated attackers may execute arbitrary commands.
 - [Affected Platforms] ASUS RT-AX55 3.0.0.4386.51598

- 6. [CVE-2025-21479] Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability (CVSS v3.1: 8.6)
 - [Ransomware Exploitation: Unknown] Multiple Qualcomm chipsets have improper authorization vulnerabilities. Executing specific command sequences may allow unauthorized instructions to run on the GPU micronode, causing memory corruption.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://docs.gualcomm.com/product/publicresources/securitybulletin/june-2025-bull
- 7. [CVE-2025-21480] Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability (CVSS v3.1: 8.6)
 - [Ransomware Exploitation: Unknown] Multiple Qualcomm chipsets have improper authorization vulnerabilities. Executing specific command sequences may allow unauthorized instructions to run on the GPU micronode, causing memory corruption.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://docs.gualcomm.com/product/publicresources/securitybulletin/june-2025-bull etin.html
- 8. [CVE-2025-27038] Qualcomm Multiple Chipsets Use-After-Free Vulnerability (CVSS v3.1: 7.5)
 - [Ransomware Exploitation: Unknown] Multiple Qualcomm chipsets have a use-afterfree vulnerability. This may cause memory corruption when rendering graphics using the Adreno GPU driver in the Chrome browser.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://docs.gualcomm.com/product/publicresources/securitybulletin/june-2025-bull etin.html
- 9. [CVE-2025-5419] Google Chromium V8 Out-of-Bounds Read and Write Vulnerability (CVSS v3.1: 8.8)
 - [Ransomware Exploitation: Unknown] Google Chromium V8 has an out-of-bounds read/write vulnerability. Remote attackers can exploit this via specially crafted HTML pages to cause heap memory corruption. This may affect multiple Chromiumbased browsers, including but not limited to Google Chrome, Microsoft Edge, and Opera.
 - [Affected Platforms] Please refer to the official list of affected versions
 - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop. html
- Affected Platforms:
 - See the affected platforms listed in the content section
- Recommended Actions:
 - 1. [CVE-2021-32030] The affected products may have reached End of Life (EoL) or End of Service (EoS). Users are advised to discontinue use.
 - 2. [CVE-2025-3935] Official patches have been released. Please update to the relevant version.
 - https://www.connectwise.com/company/trust/security-bulletins/screenconnect-secur ity-patch-2025.4
 - 3. [CVE-2025-35939] Official patches have been released. Please update to the relevant version.
 - https://github.com/craftcms/cms/releases/tag/4.15.3
 - https://github.com/craftcms/cms/releases/tag/5.7.5
 - 4. [CVE-2024-56145] Official patches have been released. Please update to the relevant

version.

- https://github.com/craftcms/cms/security/advisories/GHSA-2p6p-9rc9-62j9
- 5. [CVE-2023-39780] Upgrade the corresponding product to the following version (or higher): ASUS RT-AX55 3.0.0.4.386 53119
- 6. [CVE-2025-21479] Official patches have been released. Please update to the relevant version.
 - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bull etin.html
- 7. [CVE-2025-21480] Official patches have been released. Please update to the relevant version.
 - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bull etin.html
- 8. [CVE-2025-27038] Official patches have been released. Please update to the relevant version.
 - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bull etin.html
- 9. [CVE-2025-5419] Official patches have been released. Please update to the relevant version.
 - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.
 html

Computer and Communication Center Network Systems Division, Respectfully

From:

https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250610_02

Last update: 2025/06/10 14:32

