Posted Date: 2025/09/12

[Vulnerability Alert] CISA Added 7 Known Exploited Vulnerabilities to KEV Catalog (2025/09/01-2025/09/07)

- Subject: [Vulnerability Alert] CISA Added 7 Known Exploited Vulnerabilities to KEV Catalog (2025/09/01-2025/09/07)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000004

1. [CVE-2020-24363] TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by ransomware: Unknown] TP-Link TL-WA855RE has a vulnerability where a critical function does not have proper authentication. An unauthenticated attacker on the same network as the device could force the device to factory reset and restart by submitting a TDDP_RESET POST request. The attacker could then set a new administrator password and gain unauthorized access control. The affected products may have reached End of Life (EoL) and/or End of Service (EoS), so it is recommended that users stop using the product.
   - [Affected Platforms] TP-Link TL-WA855RE V5 versions before 200731
2. [CVE-2025-55177] Meta Platforms WhatsApp Incorrect Authorization Vulnerability (CVSS v3.1: 5.4)
   - [Exploited by ransomware: Unknown] Meta Platforms' WhatsApp has an incorrect authorization vulnerability due to incomplete authorization checks for syncing messages to a linked device. This vulnerability may allow an irrelevant user to trigger and process the content of an arbitrary URL on the target device.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://www.facebook.com/security/advisories/cve-2025-55177
3. [CVE-2023-50224] TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 6.5)
   - [Exploited by ransomware: Unknown] TP-Link TL-WR841N has an authentication bypass vulnerability by spoofing. The vulnerability is in the httpd service (default TCP port 80), which may lead to the leakage of stored credential information. The affected products may have reached End of Life (EoL) and/or End of Service (EoS). It is recommended that users stop using the product.
   - [Affected Platforms] TP-Link TL-WR841N V12
4. [CVE-2025-9377] TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability (CVSS v3.1: 7.2)
   - [Exploited by ransomware: Unknown] TP-Link Archer C7(EU) and TL-WR841N/ND(MS) have an OS command injection vulnerability in the parental control page. The affected products may have reached End of Life (EoL) and/or End of Service (EoS). It is recommended that users stop using the product.
   - [Affected Platforms]
   - TP-Link TL-WR841N/ND(MS) V9 versions before 241108
   - TP-Link Archer C7(EU) V2 versions before 241108
5. [CVE-2025-38352] Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition

Vulnerability (CVSS v3.1: 7.4)
    - [Exploited by ransomware: Unknown] The Linux kernel has a TOCTOU race condition vulnerability that has a high impact on confidentiality, integrity, and availability.
    - [Affected Platforms]
    - Linux kernel versions 2.6.36 up to but not including 5.4.295
    - Linux kernel versions 5.5 up to but not including 5.10.239
    - Linux kernel versions 5.11 up to but not including 5.15.186
    - Linux kernel versions 5.16 up to but not including 6.1.142
    - Linux kernel versions 6.2 up to but not including 6.6.94
    - Linux kernel versions 6.7 up to but not including 6.12.34
    - Linux kernel versions 6.13 up to but not including 6.15.3
    - Linux kernel version 6.16
6. [CVE-2025-48543] Android Runtime Use-After-Free Vulnerability (CVSS v3.1: 8.8)
    - [Exploited by ransomware: Unknown] Android Runtime has a use-after-free vulnerability that could lead to a Chrome sandbox escape, resulting in local privilege escalation.
    - [Affected Platforms] Please refer to the affected versions listed by the official source
    - https://source.android.com/security/bulletin/2025-09-01
7. [CVE-2025-53690] Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.0)
    - [Exploited by ransomware: Unknown] Sitecore Experience Manager(XM), Experience Platform(XP), Experience Commerce(XC), and Managed Cloud have an insecure deserialization vulnerability related to the use of a default machine key. This vulnerability may allow an attacker to achieve remote code execution using a leaked ASP.NET machine key.
    - [Affected Platforms] Please refer to the affected versions listed by the official source
    - https://support.sitecore.com/kb

- Affected Platforms:
    - For details, please refer to the Affected Platforms section in the content description.
- Recommended Measures:
1. [CVE-2020-24363] The official source has released a patch for the vulnerability; please update to the relevant version.
    - https://www.tp-link.com/us/support/download/tl-wa855re/v5/#Firmware
2. [CVE-2025-55177] The official source has released a patch for the vulnerability; please update to the relevant version.
    - https://www.facebook.com/security/advisories/cve-2025-55177
3. [CVE-2023-50224] The official source has released a patch for the vulnerability; please update to the relevant version.
    - https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware
4. [CVE-2025-9377] The official source has released a patch for the vulnerability; please update to the relevant version.
    - https://www.tp-link.com/us/support/faq/4308/
5. [CVE-2025-38352] The official source has released a patch for the vulnerability; please update to the relevant version.
    - https://git.kernel.org/stable/c/2c72fe18cc5f9f1750f5bc148cf1c94c29e106ff
    - https://git.kernel.org/stable/c/2f3daa04a9328220de46f0d5c919a6c0073a9f0b
    - https://git.kernel.org/stable/c/460188bc042a3f40f72d34b9f7fc6ee66b0b757b
    - https://git.kernel.org/stable/c/764a7a5dfda23f69919441f2eac2a83e7db6e5bb
    - https://git.kernel.org/stable/c/78a4b8e3795b31dae58762bc091bb0f4f74a2200

- https://git.kernel.org/stable/c/c076635b3a42771ace7d276de8dc3bc76ee2ba1b
- https://git.kernel.org/stable/c/c29d5318708e67ac13c1b6fc1007d179fb65b4d7
- https://git.kernel.org/stable/c/f90fff1e152dedf52b932240ebbd670d83330eca

6. [CVE-2025-48543] The official source has released a patch for the vulnerability; please update to the relevant version.
   - https://source.android.com/security/bulletin/2025-09-01
7. [CVE-2025-53690] The official source has released a patch for the vulnerability; please update to the relevant version.
   - https://support.sitecore.com/kb

Computer and Communications Center
Network Systems Group

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250912_01

Last update: **2025/09/12 14:34**