Posted Date: 2025/05/22 \

【Vulnerability Alert】 CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2025/05/12-2025/05/18)

- Subject Description: 【Vulnerability Alert】 CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2025/05/12-2025/05/18)

- Content Description:
  - Forwarded by Taiwan Computer Network Crisis Coordination Center TWCERTCC-200-202505-00000018

1. CVE-2025-47729【TeleMessage TM SGNL Hidden Functionality Vulnerability (CVSS v3.1: 4.9)
   - [Ransomware Exploitation: Unknown] TeleMessage TM SGNL has a hidden functionality vulnerability, where the archiving backend retains plaintext copies of messages from TM SGNL application users.
   - [Affected Platforms] TeleMessage archiving backend versions before 2025-05-05
2. CVE-2025-32709【Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability (CVSS v3.1: 7.8)
   - [Ransomware Exploitation: Unknown] Microsoft Windows WinSock Ancillary Function Driver has a use-after-free vulnerability, allowing authorized attackers to elevate privileges to system administrator.
   - [Affected Platforms] Please refer to the official list of affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709
3. CVE-2025-30397【Microsoft Windows Scripting Engine Type Confusion Vulnerability (CVSS v3.1: 7.5)
   - [Ransomware Exploitation: Unknown] Microsoft Windows Scripting Engine has a type confusion vulnerability, allowing unauthorized attackers to execute code on the network via specially crafted URLs.
   - [Affected Platforms] Please refer to the official list of affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30397
4. CVE-2025-32706【Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 7.8)
   - [Ransomware Exploitation: Unknown] Microsoft Windows Common Log File System driver has a heap-based buffer overflow vulnerability, allowing authorized attackers to elevate privileges locally.
   - [Affected Platforms] Please refer to the official list of affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32706
5. CVE-2025-32701【Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability (CVSS v3.1: 7.8)
   - [Ransomware Exploitation: Unknown] Microsoft Windows Common Log File System driver has a use-after-free vulnerability, allowing authorized attackers to elevate privileges locally.
   - [Affected Platforms] Please refer to the official list of affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32701

6. CVE-2025-30400Microsoft Windows DWM Core Library Use-After-Free Vulnerability (CVSS v3.1: 7.8)
    - [Ransomware Exploitation: Unknown] Microsoft Windows DWM Core Library has a use-after-free vulnerability, allowing authorized attackers to elevate privileges locally.
    - [Affected Platforms] Please refer to the official list of affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30400
7. CVE-2025-32756Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
    - [Ransomware Exploitation: Unknown] Fortinet's FortiFone, FortiVoice, FortiNDR, and FortiMail have a stack-based buffer overflow vulnerability, potentially allowing unauthorized remote attackers to execute arbitrary code or commands via specially crafted HTTP requests.
    - [Affected Platforms] Please refer to the official list of affected versions https://fortiguard.fortinet.com/psirt/FG-IR-25-254
8. CVE-2025-42999SAP NetWeaver Deserialization Vulnerability (CVSS v3.1: 9.1)
    - [Ransomware Exploitation: Unknown] SAP NetWeaver Visual Composer Metadata Uploader has a deserialization vulnerability, allowing privileged attackers to deserialize untrusted or malicious content, compromising the confidentiality, integrity, and availability of the host system.
    - [Affected Platforms] SAP NetWeaver (Visual Composer development server) VCFRAMEWORK 7.50
9. CVE-2024-12987DrayTek Vigor Routers OS Command Injection Vulnerability (CVSS v3.1: 9.8)
    - [Ransomware Exploitation: Unknown] DrayTek Vigor2960, Vigor300B, and Vigor3900 routers have an OS command injection vulnerability, originating from an unknown function in the Web management interface apmcfgupload file.
    - [Affected Platforms] Please refer to the official list of affected versions
    - https://fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.5/DrayTek_Vigor2960_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor300B/Firmware/v1.5.1.5/DrayTek_Vigor300B_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor3900/Firmware/v1.5.1.5/DrayTek_Vigor3900_V1.5.1.5_01release-note.pdf
10. CVE-2025-4664Google Chromium Loader Insufficient Policy Enforcement Vulnerability (CVSS v3.1: 4.3)
    - [Ransomware Exploitation: Unknown] Google Chromium has an insufficient policy enforcement vulnerability, allowing remote attackers to leak cross-origin data via specially crafted HTML pages.
    - [Affected Platforms] Please refer to the official list of affected versions
    - https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

- Affected Platforms:
    - Detailed content in the affected platforms section of the content description
- Recommended Measures:
    1. CVE-2025-47729 No effective mitigation measures for affected products. Users are advised to stop using related products.
    2. CVE-2025-32709 Official fixes have been released for the vulnerability, please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709

3. CVE-2025-30397【 Official fixes have been released for the vulnerability, please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30397
4. CVE-2025-32706【 Official fixes have been released for the vulnerability, please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32706
5. CVE-2025-32701【 Official fixes have been released for the vulnerability, please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32701
6. CVE-2025-30400【 Official fixes have been released for the vulnerability, please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30400
7. CVE-2025-32756【 Official fixes have been released for the vulnerability, please update to the relevant versions https://fortiguard.fortinet.com/psirt/FG-IR-25-254
8. CVE-2025-42999【 Official fixes have been released for the vulnerability, please update to the relevant versions https://me.sap.com/notes/3604119
9. CVE-2024-12987【 Official fixes have been released for the vulnerability, please update to the relevant versions
    - https://fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.5/DrayTek_Vigor2960_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor300B/Firmware/v1.5.1.5/DrayTek_Vigor300B_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor3900/Firmware/v1.5.1.5/DrayTek_Vigor3900_V1.5.1.5_01release-note.pdf
10. CVE-2025-4664【 Official fixes have been released for the vulnerability, please update to the relevant versions
    - https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

---

Computer and Communication Center
Network Systems Group