Date Posted: 2025/08/04

[Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2025/07/21-2025/07/27)

- Subject: [Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2025/07/21-2025/07/27)
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000023

1. [CVE-2025-2775] SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 9.3)
   - [Exploited by ransomware: Unknown] SysAid On-Prem has an improper restriction of XML external entity reference vulnerability in the Checkin processing function, which may allow attackers to take over administrator accounts and read arbitrary files.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://documentation.sysaid.com/docs/24-40-60
2. [CVE-2025-2776] SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 9.8)
   - [Exploited by ransomware: Unknown] SysAid On-Prem has an improper restriction of XML external entity reference vulnerability in the server URL processing function, which may allow attackers to take over administrator accounts and read arbitrary files.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://documentation.sysaid.com/docs/24-40-60
3. [CVE-2025-6558] Google Chromium ANGLE and GPU Improper Input Validation Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by ransomware: Unknown] Google Chromium has an improper input validation vulnerability in the ANGLE and GPU components, which attackers can exploit through a specially crafted HTML page to achieve sandbox escape. This vulnerability may affect multiple web browsers based on Chromium, 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/2025/07/stable-channel-update-for-desktop_15.html
4. [CVE-2025-54309] CrushFTP Unprotected Alternate Channel Vulnerability (CVSS v3.1: 9.0)
   - [Exploited by ransomware: Unknown] CrushFTP has an unprotected alternate channel vulnerability. When the DMZ Proxy feature is not enabled, the system incorrectly handles AS2 authentication, which may allow a remote attacker to obtain administrator access via HTTPS.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025
5. [CVE-2025-49704] Microsoft SharePoint Code Injection Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by ransomware: Yes] Microsoft SharePoint has a code injection vulnerability that may allow an authenticated attacker to execute arbitrary code

over the network.
    - [Affected Platforms] Please refer to the official list of affected versions
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704
6. [CVE-2025-49706] Microsoft SharePoint Improper Authentication Vulnerability (CVSS v3.1: 6.5)
    - [Exploited by ransomware: Yes] Microsoft SharePoint has an improper authentication vulnerability that may allow an authenticated attacker to perform identity spoofing over the network. If successfully exploited, attackers can view sensitive information and modify some disclosed information.
    - [Affected Platforms] Please refer to the official list of affected versions
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706

- Affected Platforms:
    - Details are in the Affected Platforms section of the Content Description
- Recommended Action:
    1. [CVE-2025-2775] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://documentation.sysaid.com/docs/24-40-60
    2. [CVE-2025-2776] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://documentation.sysaid.com/docs/24-40-60
    3. [CVE-2025-6558] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html
    4. [CVE-2025-54309] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025
    5. [CVE-2025-49704] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704
    6. [CVE-2025-49706] The official site has released a patch for the vulnerability, please update to the relevant version
        - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706

Computer and Communications Center
Network Systems Group