

Date Posted: 2025/07/10

□Vulnerability Alert□CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/06/30-2025/07/06)

- Subject: □Vulnerability Alert□CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/06/30-2025/07/06)
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000004
- 1. □CVE-2025-6543□Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
 - □Exploited by Ransomware: Unknown□ Citrix NetScaler ADC and Gateway have a buffer overflow vulnerability, which may lead to unexpected control flow changes and denial of service.
 - □Affected Platforms□Please refer to the officially listed affected versions
 - <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788>
- 2. □CVE-2025-48928□TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability (CVSS v3.1: 4.0)
 - □Exploited by Ransomware: Unknown□ TeleMessage TM SGNL has a vulnerability where a core dump file is exposed to an unauthorized control sphere. This may lead to sensitive information leakage through memory dump files containing authentication data.
 - □Affected Platforms□ TeleMessage versions up to and including 2025-05-05
- 3. □CVE-2025-48927□TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability (CVSS v3.1: 5.3)
 - □Exploited by Ransomware: Unknown□ TeleMessage TM SGNL has a vulnerability where a resource is initialized with an insecure default value. This vulnerability is related to the configuration of Spring Boot Actuator, where exposing the heap dump endpoint at /heapdump URI may lead to security risks.
 - □Affected Platforms□ TeleMessage versions up to and including 2025-05-05
- 4. □CVE-2025-6554□Google Chromium V8 Type Confusion Vulnerability (CVSS v3.1: 8.1)
 - □Exploited by Ransomware: Unknown□ Google Chromium V8 has a type confusion vulnerability, allowing remote attackers to perform arbitrary read/write operations via a specially crafted HTML page. This vulnerability may affect various web browsers that use Chromium, including but not limited to Google Chrome, Microsoft Edge, and Opera.
 - □Affected Platforms□Please refer to the officially listed affected versions
 - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html
- Affected Platforms:
 - Detailed content in the affected platforms section of the content description
- Suggested Measures:
 1. □CVE-2025-6543□ Official patches have been released for the vulnerability, please update to the relevant versions

- <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788>
- 2. [CVE-2025-48928] There are currently no effective mitigation measures for the affected products. Users are advised to stop using the relevant products.
- 3. [CVE-2025-48927] There are currently no effective mitigation measures for the affected products. Users are advised to stop using the relevant products.
- 4. [CVE-2025-6554] Official patches have been released for the vulnerability, please update to the relevant versions
 - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

Computer and Communications 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:20250710_01

Last update: **2025/07/10 16:33**

