Posted Date: 2025/09/04

[Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/08/25-2025/08/31)

- Subject: [Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/08/25-2025/08/31)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000001

1. [CVE-2025-48384] Git Link Following Vulnerability (CVSS v31: 8.0)
   - [Exploited by ransomware: Unknown] A link following vulnerability exists in Git, which stems from the inconsistent handling of carriage return characters in configuration files.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://github.com/git/git/security/advisories/GHSA-vwqx-4fm8-6qc9
2. [CVE-2024-8068] Citrix Session Recording Improper Privilege Management Vulnerability (CVSS v3.1: 8.0)
   - [Exploited by ransomware: Unknown] Citrix Session Recording has an improper privilege management vulnerability that could lead to privilege escalation to the NetworkService account access level.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://support.citrix.com/support-home/home
3. [CVE-2024-8069] Citrix Session Recording Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 8.0)
   - [Exploited by ransomware: Unknown] Citrix Session Recording has an untrusted data deserialization vulnerability that may allow limited remote code execution under NetworkService account privileges.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://support.citrix.com/support-home/home
4. [CVE-2025-7775] Citrix NetScaler Memory Overflow Vulnerability (CVSS v3.1: 9.8)
   - [Exploited by ransomware: Unknown] Citrix NetScaler ADC and NetScaler Gateway have a memory overflow vulnerability that can lead to remote code execution and/or a Denial of Service attack.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://support.citrix.com/support-home/home
5. [CVE-2025-57819] Sangoma FreePBX Authentication Bypass Vulnerability (CVSS v4.0: 10.0)
   - [Exploited by ransomware: Unknown] Sangoma FreePBX has an authentication bypass vulnerability due to insufficient validation and sanitization of user-provided input data. An attacker can access the FreePBX management interface without authentication, leading to arbitrary database operations and remote code execution.
   - [Affected Platforms] Please refer to the affected versions listed by the official source
   - https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h

- Affected Platforms:
  - For details, please refer to the Affected Platforms section in the content description.
- Recommended Measures:
  1. [CVE-2025-48384] The official source has released a patch for the vulnerability; please update to the relevant version.
     - https://github.com/git/git/security/advisories/GHSA-vwqx-4fm8-6qc9
  2. [CVE-2024-8068] The official source has released a patch for the vulnerability; please update to the relevant version.
     - https://support.citrix.com/support-home/home
  3. [CVE-2024-8069] The official source has released a patch for the vulnerability; please update to the relevant version.
     - https://support.citrix.com/support-home/home
  4. [CVE-2025-7775] The official source has released a patch for the vulnerability; please update to the relevant version.
     - https://support.citrix.com/support-home/home
  5. [CVE-2025-57819] The official source has released a patch for the vulnerability; please update to the relevant version.
     - https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h

---

Computer and Communications Center
Network Systems Group