**Date Posted: 2026/02/25**

# [Vulnerability Alert] CISA Adds 8 Known Exploited Vulnerabilities to KEV Catalog (2026/02/16-2026/02/22)

- Subject Explanation: [Vulnerability Alert] CISA Adds 8 Known Exploited Vulnerabilities to KEV Catalog (2026/02/16-2026/02/22)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000010
  - [CVE-2020-7796] Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] Synacor Zimbra Collaboration Suite (ZCS) contains a Server-Side Request Forgery vulnerability when the WebEx zimlet is installed and the zimlet JSP is enabled.
  - [CVE-2024-7694] TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 7.2)
  - [Ransomware Usage: Unknown] TeamT5 ThreatSonar Anti-Ransomware product has inadequate file content filtering. A remote attacker who has obtained product platform management privileges can upload a malicious file and execute arbitrary system commands on the server through that file.
  - [CVE-2008-0015] Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Usage: Unknown] Microsoft Windows Video ActiveX Control contains a remote code execution vulnerability. An attacker could exploit this vulnerability by constructing a specially crafted webpage. When a user browses this webpage, it may lead to remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.
  - [CVE-2026-2441] Google Chromium CSS Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Usage: Unknown] Google Chromium CSS contains a Use-After-Free vulnerability, which may allow a remote attacker to exploit heap corruption via a specially crafted HTML page. This vulnerability may affect multiple web browsers that use Chromium, including but not limited to Google Chrome, Microsoft Edge, and Opera.
  - [CVE-2021-22175] GitLab Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 6.8)
  - [Ransomware Usage: Unknown] GitLab contains a Server-Side Request Forgery vulnerability when webhook requests to the internal network are enabled.
  - [CVE-2026-22769] Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability (CVSS v3.1: 10.0)
  - [Ransomware Usage: Unknown] Dell RecoverPoint for Virtual Machines (RP4VMs) contains a use of hard-coded credentials vulnerability, which may allow unauthenticated remote attackers to gain underlying operating system access and maintain persistent access.
  - [CVE-2025-49113] RoundCube Webmail Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.9)

    - [Ransomware Usage: Unknown] RoundCube Webmail contains a deserialization of untrusted data vulnerability. Because program/actions/settings/upload.php fails to validate the _from parameter in the URL, an authenticated user can exploit this vulnerability to execute code remotely.
    - [CVE-2025-68461] RoundCube Webmail Cross-site Scripting Vulnerability (CVSS v3.1: 7.2)
    - [Ransomware Usage: Unknown] RoundCube Webmail contains a cross-site scripting vulnerability, which an attacker can exploit via the animate tag in an SVG file.
- Impacted Platforms:
    - [CVE-2020-7796] Please refer to the affected versions listed officially: https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7
    - [CVE-2024-7694] ThreatSonar Anti-Ransomware 3.4.5 and earlier versions
    - [CVE-2008-0015] Please refer to the affected versions listed officially: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-037
    - [CVE-2026-2441] Please refer to the affected versions listed officially: https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
    - [CVE-2021-22175] Please refer to the affected versions listed officially: https://about.gitlab.com/releases/2021/02/11/security-release-gitlab-13-8-4-released/
    - [CVE-2026-22769] Please refer to the affected versions listed officially: https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079
    - [CVE-2025-49113] Please refer to the affected versions listed officially: https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10
    - [CVE-2025-68461] Please refer to the affected versions listed officially: https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12
- Suggested Measures:
    - [CVE-2020-7796] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7
    - [CVE-2024-7694] Update to version 3.5.0 or later, or use Hotfix-20240715 to patch.
    - [CVE-2008-0015] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-037
    - [CVE-2026-2441] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
    - [CVE-2021-22175] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://about.gitlab.com/releases/2021/02/11/security-release-gitlab-13-8-4-released/
    - [CVE-2026-22769] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079
    - [CVE-2025-49113] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10
    - [CVE-2025-68461] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12

---

Computer and Communication Center
Network Systems Division

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

Permanent link:
**https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260225_21**

Last update: **2026/02/25 09:53**