POSTING DATE: 2026/01/29

[VULNERABILITY ALERT] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/01/19-2026/01/25)

- Subject: [VULNERABILITY ALERT] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/01/19-2026/01/25)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center (TWCERTCC) Security Alert TWCERTCC-200-202601-00000024
  - [CVE-2026-20045] Cisco Unified Communications Products Code Injection Vulnerability (CVSS v3.1: 8.2)
  - [Known to be Used in Ransomware Campaigns: Unknown] A code injection vulnerability exists in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM & P), Cisco Unity Connection, and Cisco Webex Calling Dedicated Instance. This may allow an attacker to gain user-level access to the underlying operating system and further escalate privileges to root.
  - [CVE-2025-68645] Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability (CVSS v3.1: 8.8)
  - [Known to be Used in Ransomware Campaigns: Unknown] Synacor Zimbra Collaboration Suite (ZCS) contains a PHP remote file inclusion vulnerability. This may allow a remote attacker to influence internal request distribution by sending a specially crafted request to the /h/rest endpoint, including arbitrary files within the WebRoot directory.
  - [CVE-2025-34026] Versa Concerto Improper Authentication Vulnerability (CVSS v3.1: 7.5)
  - [Known to be Used in Ransomware Campaigns: Unknown] The Traefik reverse proxy configuration of the Versa Concerto SD-WAN orchestration platform contains an improper authentication vulnerability. This may allow an attacker to access management endpoints. Internal Actuator endpoints can be exploited to obtain Heap Dumps and trace logs.
  - [CVE-2025-31125] Vite Vitejs Improper Access Control Vulnerability (CVSS v3.1: 5.3)
  - [Known to be Used in Ransomware Campaigns: Unknown] Vite Vitejs contains an improper access control vulnerability. An attacker can access unauthorized file content through specific query parameters. Only applications that expose the Vite development server to the network (using the –host or server.host configuration options) are affected.
  - [CVE-2025-54313] Prettier eslint-config-prettier Embedded Malicious Code Vulnerability (CVSS v3.1: 7.5)
  - [Known to be Used in Ransomware Campaigns: Unknown] Prettier eslint-config-prettier contains embedded malicious code. When the affected package is installed, the system executes the install.js file and launches the malicious program node-gyp.dll on Windows systems.
  - [CVE-2024-37079] Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability (CVSS v3.1: 9.8)

    - [Known to be Used in Ransomware Campaigns: Unknown] Broadcom VMware vCenter Server contains an out-of-bounds write vulnerability in its implementation of the DCERPC protocol. A malicious attacker with network access to vCenter Server may send specially crafted network packets, potentially leading to remote code execution.
- Affected Platforms:
    - [CVE-2026-20045] Please refer to the affected versions listed by the official source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b
    - [CVE-2025-68645] Please refer to the affected versions listed by the official source: https://wiki.zimbra.com/wiki/Security_Center
    - [CVE-2025-34026] Please refer to the affected versions listed by the official source: https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e
    - [CVE-2025-31125] Please refer to the affected versions listed by the official source: https://github.com/vitejs/vite/security/advisories/GHSA-4r4m-qw57-chr8
    - [CVE-2025-54313] Please refer to the affected versions listed by the official source: https://github.com/advisories/GHSA-f29h-pxvx-f335
    - [CVE-2024-37079] Please refer to the affected versions listed by the official source: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453
- Recommended Actions:
    - [CVE-2026-20045] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b
    - [CVE-2025-68645] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://wiki.zimbra.com/wiki/Security_Center
    - [CVE-2025-34026] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e
    - [CVE-2025-31125] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://github.com/vitejs/vite/security/advisories/GHSA-4r4m-qw57-chr8
    - [CVE-2025-54313] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://github.com/advisories/GHSA-f29h-pxvx-f335
    - [CVE-2024-37079] The manufacturer has released a fix for the vulnerability. Please update to the relevant version: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453

Computer and Communication Center
Network Systems Division, Respectfully