Posting Date: 2025/06/19

Vulnerability Alert CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/06/09-2025/06/15)

- Subject: Vulnerability Alert CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/06/09-2025/06/15)
- Content:
  - Forwarded from TWCERTCC-200-202506-00000011
  1. CVE-2024-42009 RoundCube Webmail Cross-Site Scripting Vulnerability (CVSS v3.1: 9.3)
     - Exploited by Ransomware: Unknown RoundCube Webmail has a cross-site scripting vulnerability that may allow a remote attacker to steal and send victims' emails through specially crafted emails by exploiting a data sanitization issue in the message_body() function in program/actions/mail/show.php.
     - Affected Platforms Please refer to the official list of affected versions.
     - https://roundcube.net/news/2024/08/04/security-updates-1.6.8-and-1.5.8
  2. CVE-2025-32433 Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 10.0)
     - Exploited by Ransomware: Unknown Erlang/OTP SSH server has a missing authentication for critical function vulnerability. This vulnerability may allow an attacker to execute arbitrary commands without providing valid credentials, leading to unauthenticated remote code execution. Malicious users can exploit vulnerabilities in the SSH protocol message handling to gain unauthorized access to affected systems. This vulnerability may affect multiple products using Erlang/OTP SSH server, including but not limited to Cisco, NetApp and SUSE.
     - Affected Platforms Please refer to the official list of affected versions.
     - https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2
  3. CVE-2025-33053 Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability (CVSS v3.1: 8.8)
     - Exploited by Ransomware: Unknown WebDAV has an external control of file name or path vulnerability. This vulnerability may allow unauthorized attackers to remotely execute code over the network. This vulnerability may affect multiple products implementing WebDAV, including but not limited to Microsoft Windows.
     - Affected Platforms Please refer to the official list of affected versions.
     - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053
  4. CVE-2025-24016 Wazuh Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.9)
     - Exploited by Ransomware: Unknown Wazuh has an untrusted data deserialization vulnerability, which can lead to remote code execution on the Wazuh server.
     - Affected Platforms Please refer to the official list of affected versions.
     - https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh
- Affected Platforms:

- Detailed content in the “Affected Platforms” section of the content description.

Computer and Communications Center
Network Systems Division