Critical Cisco Vulnerabilities Patched in Meeting Management and ClamAV

Overview

This week, Cisco released patches to address two significant vulnerabilities - a critical privilege escalation flaw in Cisco Meeting Management (CVE-2025-20156) and a heap-based buffer overflow vulnerability in ClamAV (CVE-2025-20128).

Vulnerability Breakdown

- CVE-2025-20156, CVSS 9.9 (Privilege Escalation in Cisco Meeting Management)
  - Affected Products - Cisco Meeting Management versions 3.9 and earlier.
  - Description - A flaw in the REST API allows remote, authenticated attackers with low privileges to elevate themselves to administrator.
  - Impact - Successful exploitation allows for full administrative control over edge nodes managed by Cisco Meeting Management.
  - Solution - Upgrade to version 3.9.1 or 3.10 (unaffected version). No workarounds are available.

- CVE-2025-20128, CVSS 5.3 (Heap Buffer Overflow in ClamAV)
  - Affected Products - ClamAV versions prior to 1.4.2 or 1.0.8, and Cisco Secure Endpoint Connectors for Windows, Linux, and macOS.
  - Description - Crafted OLE2 files could exploit a heap buffer overflow, terminating ClamAV's scanning process and causing a denial of service (DoS).
  - Impact - Disrupts malware detection and leaves systems vulnerable to threats.
  - Solution - Update ClamAV to versions 1.4.2 or 1.0.8.
    Upgrade Secure Endpoint Connectors to the latest fixed releases:
    - Windows - 7.5.20 or 8.4.31
    - Linux - 1.25.1
    - macOS - 1.24.4

If left unpatched, these vulnerabilities could compromise sensitive data and increase the risk of a ransomware attack.

Aspire Protects

- **Patch –** Cisco has released patches for CVE-2025-20156 and CVE-2025-20128. Please see Cisco's security advisories for patch guidance.
  - CVE-2025-20156
    - Upgrade to version 3.9.1 or migrate to version 3.10 immediately.
    - Restrict access to the REST API to trusted users.
  - CVE-2025-20128
    - Update to version 1.4.2 or 1.0.8.
    - Apply fixes to Cisco Secure Endpoint Connectors:
      - Windows - Update to 7.5.20 or 8.4.31
      - Linux - Update to 1.25.1
      - macOS - Update to 1.24.4
  - Review endpoint configurations for proper patching and disable unnecessary services.

TTPs to Watch

Privilege Escalation

- Exploit Application API [T1059.007] – The attacker may exploit flaws in the REST API to elevate privileges.

Execution

- Malicious File [T1204.002] – Crafted files targeting ClamAV may be used to disrupt endpoint scanning processes.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Based on the usage of Cisco products, potential industries could include

- Healthcare
- Finance
- Education
- Manufacturing
- Government

- Small to Medium Sized Businesses (SMBs)
- Transportation
- Retail
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Meeting Management REST API Privilege Escalation Vulnerability

ClamAV OLE2 File Format Decryption Denial of Service Vulnerability