CISCO PATCHES HIGH-SEVERITY DOS VULNERABILITIES

Vairav CVE Report

Date: April 04, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cisco has released security patches for multiple vulnerabilities affecting Meraki MX and Meraki Z series devices, Enterprise Chat and Email (ECE) appliances, Evolved Programmable Network Manager (EPNM), and Prime Infrastructure. The most critical vulnerabilities include CVE-2025-20212 and CVE-2025-20139, which could lead to denial-of-service (DoS) attacks. Additionally, Cisco warned of actively exploiting two previously patched essential vulnerabilities of Smart Licensing Utility (CVE-2024-20439 and CVE-2024-20440). Immediate patching is recommended to mitigate security risks.

VULNERABILITY DETAILS

CVE-2025-20212: Denial-of-Service Vulnerability in Cisco Meraki AnyConnect VPN Server

Description: A variable initialization issue in the AnyConnect VPN server could allow an authenticated attacker to crash the VPN server, disrupting remote connections. **Impact:** Attackers with valid VPN credentials could cause VPN disconnections, preventing new connections.

CVSS Score: 7.7 (High)

Exploitation: An attacker can exploit this flaw by sending crafted attributes during SSL VPN session establishment, leading to repeated server crashes.

Affected Products and Versions:

- Meraki MX and Meraki Z series devices running firmware versions 16.2 and 17 (must upgrade)
- Fixed in: Meraki MX firmware versions 18.107.12, 18.211.4, and 19.1.4

CVE-2025-20139: Denial-of-Service Vulnerability in Cisco Enterprise Chat and Email (ECE)

Description: Improper validation of user-supplied input in chat messaging features allows remote attackers to send malicious requests that cause the application to become unresponsive.

Impact: Service disruption, requiring administrator intervention for recovery.

CVSS Score: 7.5 (High)

Exploitation: Remote, unauthenticated attackers can send malicious chat requests to disrupt the service.

Affected Products and Versions:

- Cisco ECE with chat feature enabled
- Fixed in: Cisco ECE version 12.6 ES 10

RECOMMENDATIONS

- Apply patches immediately to affected Cisco devices and software.
- Upgrade Meraki MX firmware to 18.107.12, 18.211.4, or 19.1.4.
- Update Cisco ECE to version 12.6 ES 10 if using chat features.
- Mitigate Smart Licensing Utility risks by applying the September 2024 security update.
- Monitor Cisco security advisories for emerging threats and additional patches.
- Restrict access to VPN and chat services to prevent potential attacks.

REFERENCES

https://www.securityweek.com/vulnerabilities-expose-cisco-meraki-and-ece-products-to-dos-attacks/

https://www.cve.org/CVERecord?id=CVE-2025-20139

https://www.cve.org/CVERecord?id=CVE-2025-20212

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com