Cisco Meraki VPN Vulnerability Allows Remote Denial of Service Attacks

TL;DR

An easily exploitable Cisco Meraki AnyConnect VPN vulnerability (CVE-2025-20271) risks widespread service disruption via denial-of-service attacks. Immediate firmware updates are essential to maintain uninterrupted remote access.

Overview

This week, Cisco provided a patch for a high-severity vulnerability (CVE-2025-20271, CVSS score 8.6) impacting Cisco Meraki MX and Z Series devices using the AnyConnect VPN service with client certificate authentication enabled. An unauthenticated attacker could remotely exploit this vulnerability to trigger denial-of-service (DoS) conditions.

Affected Products

CVE-2025-20271 affects multiple Cisco Meraki MX and Z Series models if running susceptible firmware versions and using client certificate authentication for AnyConnect VPN, including:

- MX64, MX64W, MX65, MX67 series, MX68 series, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600, vMX
- Z3, Z3C, Z4, Z4C

The vulnerability stems from errors in variable initialization during the establishment of SSL VPN sessions. Attackers exploiting this vulnerability can send specifically crafted HTTPS requests causing the Cisco AnyConnect VPN service to restart abruptly. This disruption immediately disconnects all active VPN sessions, forcing users to reauthenticate. Continuous exploitation could lead to prolonged outages, preventing new VPN connections.

Although Cisco has stated that there is no evidence of active exploitation or public use of the vulnerability, CVE-2025-20271 is easy for attackers to exploit. Given the importance of VPN services, Aspire recommends that organizations patch as soon as possible.

Aspire Protects

- **Patch** – Organizations should immediately upgrade affected devices to fixed firmware versions (18.107.13, 18.211.6, or 19.1.8). See Cisco's advisory for guidance.
- Regularly monitor VPN logs for unusual activity.
- Schedule upgrades for unsupported models (MX400 and MX600), as they will not receive security patches due to end-of-life status.

TTPs to Watch

Impact

- Endpoint Denial of Service [T1499] – Malformed HTTPS requests crash and restart the AnyConnect service, dropping active sessions.

Impact

- Network Denial of Service: Direct Network Flood [T1498.001] – Repeated exploit attempts can mimic a flood, keeping VPN access offline.

IoCs

There are no known IoCs associated with the above vulnerability 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

Organizations across various sectors relying heavily on secure VPN services may be particularly vulnerable, including:

- Education
- Healthcare
- Retail and eCommerce
- Government
- Finance
- Education
- Manufacturing
- Technology

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

NVD - CVE-2025-20271

Cisco Meraki MX and Z Series AnyConnect VPN with Client Certificate Authentication Denial of Service Vulnerability