CVE-2025-20271: Denial of Service in Cisco AnyConnect VPN Server

Vairav CVE Report

Date: June 24, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148

Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A high-severity vulnerability, **CVE-2025-20271**, has been identified in the Cisco AnyConnect VPN server component on Cisco Meraki MX and Z Series Teleworker Gateway devices. If exploited, this flaw allows an unauthenticated, remote attacker to trigger a denial-of-service (DoS) condition causing the VPN service to crash and restart resulting in a complete disruption of secure remote access. The vulnerability carries a **CVSS score of 8.6 (High)**.

VULNERABILITY DETAILS

CVE-2025-20271

- **Description:** During SSL VPN session establishment for AnyConnect using *client certificate authentication*, a variable initialization error can occur. An attacker can exploit this by sending a sequence of specially crafted HTTPS requests to the VPN endpoint. This inconsistency in handling uninitialized variables leads to a crash and restart of the AnyConnect VPN service.
- **Impact:** This vulnerability forces all active SSL VPN sessions to drop, requiring re-authentication. A sustained attack prevents new SSL VPN connections, fully denying remote access. It is particularly disruptive in remote or hybrid work environments reliant on Meraki VPN gateways.
- **CVSS Score:** 8.6 (High)

AFFECTED VERSIONS

The following Cisco Meraki MX and Cisco Meraki Z Series devices are affected if they have Cisco AnyConnect VPN with client certificate authentication enabled.

- **Cisco Meraki MX Series:**
  - MX64
  - MX64W
  - MX65
  - MX65W
  - MX67
  - MX67C

  - MX67W
  - MX68
  - MX68CW
  - MX68W
  - MX75
  - MX84
  - MX85
  - MX95
  - MX100
  - MX105
  - MX250
  - MX400
  - MX450
  - MX600
  - vMX
- **Cisco Meraki Z Series:**
  - Z3
  - Z3C
  - Z4
  - Z4C

EXPLOIT DETAILS

This vulnerability particularly concerns environments where Cisco AnyConnect VPN is enabled with client certificate authentication. A possible attack scenario looks like this:

1. Attacker identifies deployed Meraki endpoint with the vulnerable configuration.
2. Sends crafted HTTPS requests targeting the SSL VPN session routine.
3. Server crashes, restarting VPN service leading to current sessions being dropped.
4. With sustained requests, new SSL VPN sessions fail leading to complete DoS.

RECOMMENDED ACTIONS

Patch & Upgrade

Cisco has released firmware updates to address this vulnerability. Users are advised to upgrade to the following fixed versions:

- Cisco Meraki MX Firmware Release 18.1xx: Upgrade to 18.107.13 or later.
- Cisco Meraki MX Firmware Release 18.2xx: Upgrade to 18.211.6 or later.
- Cisco Meraki MX Firmware Release 19.1: Upgrade to 19.1.8 or later.

ADDITIONAL SECURITY MEASURES

- **Access Control:** Restrict management interfaces and VPN endpoints to trusted IPs (VPN concentrators, firewall ACLs).
- **Detection & Monitoring:** Enable logging and alerting for unusual SSL session restarts, repeated session failures, or spikes in connection attempts.
- **Layered Network Segmentation:** Place VPN concentrators behind IDS/IPS and web application firewalls capable of blocking anomalous HTTP/HTTPS patterns.
- **Graceful Session Handling:** Implement rate limiting or connection throttling to reduce the impact of repeated exploit attempts.
- **Patch Management Policy:** Ensure device firmware is updated promptly after vendor advisories, and develop a validation/testing plan before deploying updates.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-20271
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

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