CVE-2025-20212: Denial of Service in Cisco AnyConnect

Vairav CVE Report

Date: April 8, 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

A vulnerability, identified as **CVE-2025-20212**, has been discovered in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series devices. This vulnerability allows an authenticated, remote attacker to cause a denial of service (DoS) condition in the Cisco AnyConnect service. The vulnerability has a **CVSS score of 7.7 (High)**. If exploited, this vulnerability could lead to service disruption, requiring remote users to reauthenticate.

VULNERABILITY DETAILS

CVE-2025-20212

- **Description:** This vulnerability exists due to an uninitialized variable when an SSL VPN session is established. An authenticated, remote attacker with valid VPN user credentials can exploit this by supplying crafted attributes during the SSL VPN session establishment, causing the Cisco AnyConnect VPN server to restart unexpectedly.
- **Impact:** Successful exploitation results in a denial of service (DoS) condition, leading to the termination of active SSL VPN sessions and forcing remote users to initiate new VPN connections and reauthenticate.
- **CVSS Score:** 7.7 (High)

AFFECTED PRODUCTS

The following Cisco Meraki MX and Cisco Meraki Z Series devices are affected if they have Cisco AnyConnect VPN 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

In environments where Cisco Meraki MX and Z Series devices are deployed to provide VPN services via the Cisco AnyConnect VPN server, an authenticated attacker with valid VPN credentials can exploit this vulnerability by sending crafted attributes during the SSL VPN session establishment. This action causes the VPN server to restart, disrupting active VPN sessions and requiring users to reauthenticate, thereby leading to potential service outages and reduced availability of VPN services.

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 18.1: Upgrade to release 18.107.12 or later.
- Cisco Meraki MX Firmware Release 18.2: Upgrade to release 18.211.4 or later.
- Cisco Meraki MX Firmware Release 19.1: Upgrade to release 19.1.3 or later.

ADDITIONAL SECURITY MEASURES

- **Restrict VPN Access**: Limit VPN access to only those users who require it, and regularly review user access privileges to minimize potential attack vectors.
- **Monitor VPN Activity**: Implement monitoring to detect unusual VPN activity, such as frequent session drops or unexpected reauthentication requests, which may indicate exploitation attempts.
- **Incident Response Plan**: Develop and maintain an incident response plan to address potential DoS attacks, ensuring quick recovery and minimal service disruption.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-20212
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vNRpDvfb#fs

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