Cisco Meraki VPN Flaw May Allow Session Takeover or Disruption

Overview

There is a Cisco vulnerability (CVE-2024-20509, CVSS 5.8) affecting Meraki MX and Z Series devices running the AnyConnect VPN service. The flaw could let unauthenticated remote attackers hijack active VPN sessions or prevent users from connecting, simply by guessing authentication handlers and sending crafted HTTPS requests.

TL;DR

A flaw (CVE-2024-20509, CVSS 5.8) in Cisco Meraki MX and Z Series devices running AnyConnect VPN could allow attackers to hijack sessions or block access. No user interaction required. Patch now if you're running firmware 16.2+ or later.

Affected Products

- 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
    - *Conditions – Devices must be running firmware 16.2 or later with AnyConnect VPN enabled.*

This flaw stems from two issues, weak entropy used during the authentication process and a race condition in how handlers are managed. Together, they create an opening where an attacker can guess the session handler values with enough precision to either hijack a user's VPN session or block them from connecting altogether. No authentication is required to exploit this flaw, just carefully crafted traffic sent to an affected device.

VPN hijacking without credentials is a major concern in remote-work-heavy environments. While this vulnerability isn't critical, it's an easy vulnerability to exploit. Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Upgrade to a fixed firmware version
    - 18.1 - update to 18.107.13

    - 18.2 - update to 18.211.3
- Disable AnyConnect VPN temporarily if patching is not immediately possible (test impact first).
- Monitor for unexpected VPN session drops or behavior until patching is complete.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have exploited the public VPN interface to guess session handler values and hijack user sessions or deny service.

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

This vulnerability may impact organizations that rely heavily on remote access infrastructure through Cisco Meraki devices.

- Healthcare
- Public Sector
- Retail
- Finance
- Education
- Professional Services

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 Meraki MX and Z Series Teleworker Gateway AnyConnect VPN Session Takeover and Denial of Service Vulnerability