مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Cisco Meraki Gateway AnyConnect VPN DoS Vulnerabilities

Tracking #:432316472

Date:05-11-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been discovered in the Cisco AnyConnect VPN server of Cisco Meraki MX and Z Series Teleworker Gateway devices, which could allow unauthenticated, remote attackers to cause a denial of service (DoS) condition on the affected devices.

## TECHNICAL DETAILS:

Multiple vulnerabilities have been discovered in the Cisco AnyConnect VPN server of Cisco Meraki MX and Z Series Teleworker Gateway devices, which could allow unauthenticated, remote attackers to cause a denial of service (DoS) condition on the affected devices. These vulnerabilities could disrupt VPN services by forcing the Cisco AnyConnect VPN server to restart or preventing new VPN connections from being established.
The vulnerabilities affect various models of Cisco Meraki MX Series and Z Series devices running vulnerable firmware versions with AnyConnect VPN enabled. The most severe vulnerabilities have a CVSS base score of 8.6, indicating a high severity level.

**Key Vulnerabilities:**

1. **CVE-2024-20498, CVE-2024-20499, CVE-2024-20501**:
    - Impact: DoS condition in AnyConnect service
    - Vector: Crafted HTTPS request to VPN server
    - Effect: VPN server restart, connection failures
    - CVSS Score: 8.6 (High)
2. **CVE-2024-20500**:
    - Impact: DoS condition preventing new VPN connections
    - Vector: Crafted TLS/SSL messages
    - Effect: VPN server stops accepting new connections
    - CVSS Score: 5.8 (Medium)
3. **CVE-2024-20502**:
    - Impact: DoS condition preventing new VPN connections
    - Vector: Crafted HTTPS requests
    - Effect: VPN server stops accepting new connections
    - CVSS Score: 5.8 (Medium)
4. **CVE-2024-20513**:
    - Impact: Targeted DoS for specific VPN users
    - Vector: Brute-forcing or predicting session handlers
    - Effect: Termination of targeted VPN sessions
    - CVSS Score: 5.8 (Medium)

**Affected Products**

The following products are impacted if running a vulnerable release of Cisco Meraki MX firmware with AnyConnect VPN enabled:

- **Meraki MX Series**: MX64, MX64W, MX65, MX65W, MX67, MX67C, MX67W, MX68, MX68CW, MX68W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600
- **Meraki Z Series**: Z3, Z3C, Z4, Z4C

**Fixed Releases:**

| Cisco Meraki MX Firmware Release | First Fixed Release |
|---|---|
| Earlier than 16.2 | Not affected. |
| 16.2 and later | Migrate to a fixed release. |
| 17.0 and later | Migrate to a fixed release. |
| 18.0 and later | 18.211.2 |

## RECOMMENDATIONS:

- Upgrade Affected Devices to the latest fixed firmware releases for the impacted devices.
- Disable AnyConnect VPN as a Temporary Mitigation: While disabling the AnyConnect VPN will remove the attack vector, this is a temporary workaround and may impact users' ability to connect remotely. Disabling the VPN should be considered only until the upgrade can be applied.
- Monitor Devices for Abnormal Behavior: Administrators should actively monitor their networks for signs of attacks attempting to exploit these vulnerabilities. Look for unusual or sustained VPN connection failures and investigate logs for any signs of suspicious activity.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2