Post Date: 2025/06/26

□Vulnerability Alert□Cisco recently released updates to address security vulnerabilities in Meraki MX, it is recommended that administrators evaluate and update as soon as possible!

* Subject: □Vulnerability Alert□Cisco recently released updates to address security vulnerabilities in Meraki MX, it is recommended that administrators evaluate and update as soon as possible!

* Content:

- Forwarded from Chunghwa Telecom CHTSECURITY-200-202506-00000001
- CVE-2025-20271: CVSS 8.6 An unauthenticated remote attacker could exploit this vulnerability by sending crafted HTTPS requests to an affected device. This could lead to a restart of the Cisco AnyConnect VPN server, causing termination of all existing SSL VPN sessions, preventing the establishment of new VPN connections, and ultimately, rendering the VPN service unavailable to legitimate users.

* Affected Platforms:

- Meraki MX

* Suggested Actions:

- Please refer to Cisco's official website for instructions and suggested actions:

1. Meraki MX firmware version 18.107.13 (and later)
2. Meraki MX firmware version 18.211.6 (and later)
3. Meraki MX firmware version 19.1.8 (and later)

* References:

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20271
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

Computer and Communications Center
Network Systems Group