Cisco ASA and FTD Software Vulnerability Under Active Exploitation

Overview

Cisco released patches to address a vulnerability that is under active exploitation within its Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software. Tracked as CVE-2024-20481 (CVSS 5.8), this vulnerability targets the Remote Access VPN (RAVPN) service, allowing unauthenticated attackers to induce a denial-of-service (DoS) condition through resource exhaustion.

The vulnerability causes a DoS condition in the RAVPN service of ASA and FTD, potentially requiring a device reload for full service restoration. It can be exploited by sending a large volume of VPN authentication requests, leading to resource depletion. CVE-2024-20481 has been actively targeted in widespread brute-force attacks.

Affected Products

- Cisco ASA Software (all versions)
- Cisco Firepower Threat Defense (FTD) Software (all versions up to the latest)

In addition to releasing patches for CVE-2024-20481, Cisco also released patches for the other critical vulnerabilities with the potential for arbitrary command execution and unauthorized access:

- CVE-2024-20424 (CVSS 9.9) - Command injection in FMC's web-based interface.
- CVE-2024-20329 (CVSS 9.9) - Command injection in ASA's SSH subsystem.
- CVE-2024-20412 (CVSS 9.3 - Static credentials present in certain Firepower device models.

Leaving CVE-2024-20481 unpatched could result in the exposure of sensitive data and internal resources. Aspire recommends patching immediately to help mitigate the risk of exploitation.

Aspire Protects

- **Patch –** Immediate patching is highly recommended. Please see Cisco's advisory for CVE-2024-20481. You may find patch guidance for the other vulnerabilities in the links below:
  - CVE-2024-20329
  - CVE-2024-20424
  - CVE-2024-20412
- To check your Cisco software for vulnerabilities, please use Cisco's Software Checker.

IoCs

- There are no known IoCs associated with the above vulnerabilities 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.

TTPs to Watch

Initial Access

- Brute-Force Attack (T1110) – Attackers leverage brute-force password spraying attacks, overwhelming VPN and SSH authentication.

Persistence

- Resource Exhaustion (T1499) – High-frequency authentication requests deplete device memory and processing power, impacting RAVPN availability.

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 cyberattacks.
- **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 Adaptive Security Appliance and Firepower Threat Defense Software Remote Access VPN Brute Force Denial of Service Vulnerability

Cisco Secure Firewall Management Center Software Command Injection Vulnerability

Cisco Adaptive Security Appliance Software SSH Remote Command Injection Vulnerability

Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series Static Credential Vulnerability