Cisco Firepower 3100/4200 Vulnerability Could Block Encrypted Connections

TL;DR

Cisco released updates for a denial-of-service vulnerability (CVE-2025-20127, CVSS 7.7) in Cisco Secure Firewall ASA and FTD running on Firepower 3100/4200 Series devices.

*The flaw in the TLS 1.3 cipher **TLS_CHACHA20_POLY1305_SHA256** can block all new encrypted connections until the device is rebooted. Workarounds and patches are available.*

Overview

Cisco disclosed CVE-2025-20127, a high-severity vulnerability (CVSS 7.7) in Secure Firewall ASA and FTD software on Firepower 3100 and 4200 hardware. Successful exploitation prevents the device from establishing new SSL/TLS or VPN connections, including management traffic. Once in this failed state, the only way to restore functionality is to reload the appliance.

CVE-2025-20127 allows a remote, authenticated attacker to trigger a denial-of-service condition in Cisco Secure Firewall ASA and FTD software when the TLS 1.3 cipher ***TLS_CHACHA20_POLY1305_SHA256*** is enabled. By generating a large number of TLS 1.3 connections, the attacker depletes resources required to process encrypted traffic. As a result, the device will refuse any new SSL/TLS or VPN requests until it is rebooted. Only Firepower 3100 and 4200 appliances running ASA or FTD are impacted. Cisco Secure Firewall Management Center (FMC) is not affected.

If this vulnerability is exploited, VPNs and other encrypted connections could stop working, cutting off users and admins. The device has to be rebooted to recover, which means downtime is guaranteed. In larger environments, an attacker could take out multiple firewalls at once, causing wider outages. Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Apply Cisco's patch. See Cisco's advisory for details.
- Temporary workaround – Remove the cipher with no ssl cipher tlsv1.3 custom.
- Monitor for SSL errors and rising HANDLE_ALLOC_FAILED counters.
- Reload affected devices if they enter the failed state.

TTPs to Watch

Impact

- Resource Hijacking [T1499] – The attacker may exhaust TLS processing resources.

Impact

- Service Stop [T1489] – The attacker can force the device offline until rebooted.

IoCs

Look for repeating SSL error logs such as:

- *error:1424A044:SSL routines:write_state_machine:internal*
- *error@libssl_ext_hndshk_accel.c:87*

check for rapidly increasing values in the HANDLE_ALLOC_FAILED counter by running the command:

- *show counters | include HANDLE_ALLOC_FAILED*

Targeted Industries

This vulnerability impacts any organization operating Cisco Secure Firewall ASA or FTD appliances in production environments.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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 Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 3100 and 4200 Series TLS 1.3 Cipher Denial of Service Vulnerability

NVD - CVE-2025-20127