Cisco Firepower 2100 ASA/FTD IPv6 VPN Processing Flaw Causes DoS

TL;DR

Cisco disclosed CVE-2025-20222, a high-severity (CVSS 8.6) denial-of-service flaw in Firepower 2100 Series running ASA or FTD Software.

An unauthenticated remote attacker could trigger a device reload by sending IPv6 packets over an IPsec VPN. No workarounds exist, but Cisco has released patched software.

Overview

There is a vulnerability in Cisco's RADIUS proxy feature of the IPsec VPN on Firepower 2100 Series devices. Improper handling of IPv6 packets can be abused by a remote, unauthenticated attacker to reload the device, resulting in loss of service.

Affected Products

- Cisco Firepower 2100 Series running ASA or FTD software with all of the following:
  - IPsec VPN (IKEv1 or IKEv2) enabled
  - IPv6 enabled on the interface handling RADIUS traffic
  - ACL configured to permit IP traffic (ASA 9.16 or earlier, FTD 7.0 or earlier)

Products outside the Firepower 2100 Series, and Cisco Secure Firewall Management Center (FMC), are not affected.

CVE-2025-20222 has a CVSS score of 8.6. Exploitation requires only the ability to send IPv6 traffic over an active IPsec VPN connection. The flaw leads to a device reload, creating a denial-of-service condition. This vulnerability could be extremely disruptive for organizations relying on Firepower 2100 devices. Cisco has confirmed there are no workarounds, but software updates are available.

Aspire Protects

- **Patch** - Apply Cisco's patch as soon as possible. See Cisco's advisory for further details.
- Use Cisco's Software Checker to validate whether your device and release are impacted.
- Review VPN, IPv6, and ACL settings to ensure they align with Cisco's guidance.

TTPs to Watch

Impact

- Endpoint Denial of Service [T1499] – The attacker may force repeated device reloads, disrupting availability.

Impact

- Network Denial of Service [T1498] – The attacker may send crafted IPv6 packets over IPsec to exhaust resources and interrupt VPN traffic.

Targeted Industries

This vulnerability impacts any organization running Cisco Firepower 2100 Series devices with ASA or FTD software configured for IPsec VPN and IPv6.

- 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 2100 Series IPv6 over IPsec Denial of Service Vulnerability

NVD - CVE-2025-20222