# UPDATE: Cisco Firewall Zero-Days Under Active Exploitation

*Two zero-day vulnerabilities in Cisco ASA and FTD are being actively exploited. CVE-2025-20333 (CVSS 9.9) allows attackers with valid VPN credentials to achieve remote code execution as root.*

*CVE-2025-20362 (CVSS 6.5) allows unauthenticated access to restricted URLs. Cisco has released patches and there are no workarounds.*

## *UPDATE – 11/6/2025*

Cisco reported a new variant exploiting CVE-2025-20333 in the VPN web server of ASA/FTD. Attackers with valid VPN credentials send crafted HTTP(S) requests that take advantage of improper input validation. This can run arbitrary code as root, or force the device to reload, causing a denial of service. Cisco confirmed active exploitation in the wild. Because there's a confirmed new attack variant causing device reloads (DoS), it's strongly advised to prioritize patching. Previous recommendations in Aspire's original Emergency Flash Notice remain in effect and should continue to be followed. See details below.

---

## Overview

Cisco confirmed that attackers are exploiting two zero-day flaws in ASA and FTD firewall software. Both issues affect the VPN web server component, and there are no mitigations beyond upgrading to fixed releases.

### Vulnerability Breakdown

- CVE-2025-20333 (CVSS 9.9) – This is in the VPN web server of Cisco Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD). If exploited, an attacker with valid VPN credentials can run arbitrary code as root on the firewall. That means full compromise of the firewall itself.

- CVE-2025-20362 (CVSS 6.5) – This is also in the VPN web server of ASA/FTD. It lets an unauthenticated attacker access restricted URLs without logging in. Again, this affects the firewall directly, since ASA and FTD are firewall platforms that sit on the network edge.

### Affected Products

- Cisco ASA with AnyConnect IKEv2, Mobile User Security, or SSL VPN enabled

- Cisco FTD with AnyConnect IKEv2 or SSL VPN enabled

ASA and FTD platforms are a consistent target for both state-backed groups and financially motivated threat actors. Aspire recommends patching immediately.

## Aspire Protects

- **Patch** – Updates are available for CVE-2025-20333 and CVE-2025-20362 and patch guidance can be found in Cisco's security advisory. Customers should verify exposure using the Cisco Software Checker.
- Limit or disable VPN features not in use until patching is complete.
- Monitor VPN logs and web access requests for unusual or repeated activity.

### TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers may target exposed ASA/FTD VPN web servers with crafted HTTPS requests.

Execution

- Exploitation for Client Execution [T1203] – CVE-2025-20333 allows remote code execution as root.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Successful exploitation grants full system control.

### IoCs

At this time, Cisco has not released IoCs related to exploitation of CVE-2025-20333 or CVE-2025-20362. However, there are behavioral IoCs organizations should monitor for:

- Unusual or repeated HTTPS requests to ASA/FTD VPN web servers
- Unauthorized attempts to access restricted URL endpoints
- Spikes in failed VPN logins or abnormal webvpn activity

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.

**Targeted Industries**

These flaws impact any organization running Cisco ASA or FTD firewalls in production environments:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Government
- 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 Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability

Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability