Actively Exploited Cisco ASA and FTD Vulnerability Can Crash Firewalls

Author: Portia S. Cole – CTI Researcher

TL;DR

Cisco confirmed active exploitation of CVE-2026-20349, a high-severity vulnerability affecting the Remote Access SSL VPN service in Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software.

An unauthenticated attacker can send a crafted HTTP request that forces an affected device to reload, resulting in a denial-of-service condition.

Overview

There is a high-severity vulnerability (CVE-2026-20349, CVSS 8.6) in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance Software and Cisco Secure Firewall Threat Defense Software. These products provide firewall, VPN and threat protection capabilities for enterprise networks.

The vulnerability is caused by insufficient error checking when the service processes HTTP requests. An unauthenticated attacker can exploit it remotely by sending a crafted request to an affected device. Successful exploitation causes the firewall to reload unexpectedly, interrupting VPN access and network security services.

The Cybersecurity and Infrastructure Security Agency added CVE-2026-20349 to its Known Exploited Vulnerabilities Catalog on August 11, 2026. No threat actor or specific exploitation campaign has been publicly identified.

Cisco released hot fixes for supported Adaptive Security Appliance and Secure Firewall Threat Defense versions. There are no workarounds.

Affected Products

The vulnerability affects devices running vulnerable versions of:

- Cisco Secure Firewall Adaptive Security Appliance Software
- Cisco Secure Firewall Threat Defense Software

Devices are vulnerable when at least one of the following features is enabled:

- IKEv2 Remote Access VPN with client services
- SSL VPN
- Zero Trust Network Access in Secure Firewall Threat Defense Software

Cisco Secure Firewall Management Center Software is not affected.

Aspire Protects

- **Patch** – Install the Cisco hot fix for the affected Adaptive Security Appliance or Secure Firewall Threat Defense release. Cisco has not provided a workaround. See Cisco's advisory for more information.
- Use the Cisco Software Checker and review device configurations for enabled IKEv2 Remote Access VPN client services, SSL VPN or Zero Trust Network Access.
- Remediate affected firewalls with externally accessible Remote Access SSL VPN services first.
- Investigate unexpected firewall reloads, crash information and service interruptions. Review Remote Access SSL VPN activity immediately before each event.
- Confirm that applicable Cisco Snort rules 46897 and 59654 are available and enabled.

TTPs to Watch

Impact

- Application or System Exploitation – T1499.004: Threat actors exploit CVE-2026-20349 by sending a crafted HTTP request to the Remote Access SSL VPN service. Successful exploitation causes the affected Cisco firewall to reload, resulting in a denial-of-service condition.

IoCs

There are no known IoCs 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.

Targeted Industries

Organizations in any sector may be affected if they operate vulnerable Cisco firewalls with exposed remote-access services, including:

- Government
- Technology
- Healthcare
- Finance
- Education
- Retail
- Manufacturing

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 Remote Access SSL VPN Denial of Service Vulnerability