Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Firewall Zero-Day Lets Anyone Reboot Your VPN

Date of Publication	Admiralty Code	TA Number
October 30, 2026	A1	TA2026320

Summary

First Seen: October 2026
Affected Products: Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software
Impact: Cisco has disclosed CVE-2026-76418, a high-severity zero-day in the Remote Access SSL VPN service of Cisco Secure Firewall ASA and FTD software. An unauthenticated, remote attacker can send a crafted request to an exposed SSL VPN login service and force the firewall to reload, taking the device offline and cutting remote access for everyone behind it. No login is needed to reach the flawed code, so anyone who can get to the VPN service over the network can attempt it. Cisco PSIRT found attackers already using the flaw during October 2026 and published its advisory on October 28, 2026 along with fixed software. No threat actor has been named and no malware has been tied to the attacks so far. Cisco has not linked the flaw to remote code execution or data theft, so the damage is downtime rather than a compromised device, but an attacker who can restart a VPN gateway at will can keep remote staff, administrators, and partners locked out.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-76418	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability	Cisco Secure Firewall ASA Software, Cisco Secure Firewall Threat Defense (FTD) Software	✓	✓	✓

Vulnerability Details

#1

CVE-2026-76418 is a denial-of-service flaw in the Remote Access SSL VPN service of Cisco Secure Firewall ASA and FTD software. Cisco classifies it as CWE-690, an unchecked return value that leads to a NULL pointer dereference. The software makes a call, never checks whether it worked, and uses the result anyway. When that result is empty, the appliance crashes and reloads.

#2

The flaw only shows up when secondary authentication is set on a tunnel group. An attacker sends a crafted request while connecting to the SSL VPN, and the faulty code path crashes the device. No VPN login is needed to get there, so the attacker needs no credentials, only network access to the login service.

#3

A device is exposed when three things are true at once: it runs an affected ASA or FTD release, its SSL VPN login service is reachable, and secondary authentication is set on an affected tunnel group. Cisco warns that checking only the profiles shown on the login page is not enough, and that switching off the tunnel group list does not help if DefaultWEBVPNGroup still uses secondary authentication. Fixed ASA releases begin at 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, and 9.24.1.27 or 9.24.10.1. Fixed FTD releases begin at 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, and 10.1.1. Cloud-delivered Firewall, Cloud-delivered Firewall Management Center, Secure Access, and Secure Firewall Management Center are not affected.

#4

Exploitation confirmed attacks during October 2026 but has named no attacker or victim. There is no public exploit code and no published indicators, so hunting should focus on behaviour and configuration rather than static IoCs. The missing exploit code is no reason to delay, since attacks were already happening before disclosure.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-76418	Cisco Secure Firewall ASA Software (Before 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 / 9.24.10.1); Cisco Secure Firewall Threat Defense (FTD) Software (Before 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, 10.1.1)	cpe:2.3:a:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*	CWE-690

Recommendations

Upgrade to the Fixed Release Now: Move affected ASA and FTD appliances to the fixed release that matches your branch, starting with 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, or 9.24.1.27 for ASA and 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, or 10.1.1 for FTD. Cisco has confirmed there is no workaround that fully fixes the flaw, so patching is the only real remedy. Use the Cisco Software Checker and the compatibility guides to pick the correct release for your hardware and current software branch.

Confirm Whether You Are Actually Exposed: Check whether SSL remote access VPN is enabled, which on ASA means a running configuration containing the webvpn keyword with SSL VPN enabled on at least one interface, and on FTD means reviewing the deployed Remote Access VPN policy through Secure Firewall Management Center or Device Manager. Then inspect every tunnel group, including DefaultWEBVPNGroup, for secondary-authentication-server-group. Do not limit the review to the profiles that appear in the group list on the login page, because the exposure is not limited to what users can see.

Apply Cisco's Temporary Mitigation Only If You Cannot Patch Yet: If DefaultWEBVPNGroup does not use secondary authentication, you can disable the tunnel group list with the no tunnel-group-list enable command, which means users will need to know their correct connection profile instead of choosing it from a list. If DefaultWEBVPNGroup does use secondary authentication, removing it with no secondary-authentication-server-group closes the path but lowers the authentication strength of your remote access VPN. Treat either change as a short-term stopgap, test it before rolling it out, and reverse it once the upgrade is in place.

Prioritise by Real-World Exposure: Patch internet-facing appliances first, especially those running vulnerable releases, serving SSL remote access VPN, using secondary authentication, and carrying critical remote workforce or administrative connectivity. Check whether high availability or failover can keep service running while you upgrade, so the maintenance window itself does not create the outage you are trying to prevent.

Review Logs for Unexplained Reloads: Go back through system logs for the period before patching and look for appliance reloads with no maintenance or administrative explanation, firewall uptime resetting unexpectedly, repeated SSL VPN connection attempts just before a restart, clusters of abnormal remote access requests from external infrastructure, and unusual authentication activity around the restarts. Several unexplained reloads in a short window is a particularly strong signal worth running down.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 30, 2026 • 07:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com