CVE-2026-76418 / ASSIGN AND VERIFY

# Could this VPN interrupt the work that depends on it?

Complete with the firewall owner. Record decisions and references, not passwords or raw configuration dumps. Keep the completed sheet within your team.

**Device or pair / site alias**

**Owner / contact route**

**Product / running branch and build**

**Checked at / time zone**

## 01 Establish the affected configuration

SSL remote-access VPN service enabled and reachable?

[ ] Yes [ ] No [ ] Unknown / owner to verify

Is `tunnel-group-list enable` configured?

### Yes: check all groups

Include DefaultWEBVPNGroup and profiles not displayed in the list. Look for secondary authentication.

### No: check the default

Check DefaultWEBVPNGroup. Removing the list alone does not clear exposure when this group uses secondary authentication.

**Secondary authentication in relevant scope / policy or config reference**

On FTD, review the deployed VPN policy and resulting running configuration in FMC or FDM.

## 02 Match and verify the supported fix

**Exact branch / vendor target / checker reference**

**Change owner / window / ticket**

**Running build after change / checked at**

**Other applicable members verified / by whom**

**Use the correct fix for each software branch.**

A later branch is not cleared by an earlier branch's version minimum. Cisco's conditional mitigations can reduce VPN security; evaluate the full vendor instructions with the responsible owners.

Vendor advisory and current fixed-release matrix:
Cisco CVE-2026-76418 advisory. First publication October 28, 2026. CISA KEV addition October 29; catalog federal due date November 1. Sources checked October 30.

CVE-2026-76418 / DEPENDENCY AND EVIDENCE

# Give the outage a timeline and a response owner.

**Remote task / service dependent on this VPN**

**Recovery owner / alternate contact path**

**Failover behavior checked / result or gap**

**Approved recovery approach / reference**

## 03 Preserve and compare the records

### Appliance and collector

Startup/reload time, uptime, external syslog, crash artifacts, time zone and clock state, collector/source identity.

### Context outside the appliance

Change ticket, power/monitoring alerts, peer behavior, nearby VPN session and authentication records where retained.

| Record / time window | Retained location or case reference | Owner / next check |
|---|---|---|
| Startup or restart evidence | | |
| Crash / support evidence | | |
| VPN / authentication context | | |
| Change / power / peer context | | |

> **A startup log is a symptom, not the cause.**
>
> The supplied hunts find documented startup messages. One restart may produce more than one record. Missing records can mean a collection gap. Check the device and independent context before deciding what happened.

## 04 Close the handoff, or name the gap

### What explains the restart, and what still needs checking?

**Case / Cisco TAC reference / next action**

**Owner / due time / alternate route**

Preserve evidence before avoidable resets or cleanup. A reload does not prove this exploit, and fixing this DoS does not rule out other compromise. No exploit test is needed to complete this sheet.

Guide and hunt starters:
https://deceptioncheck.ai/blog/cisco-vpn-restart-before-login.