contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software exploited

CVE-2026-76418 · on CISA's exploited list since 29 October 2026

Analysis Report

Organisations running Cisco ASA or FTD with SSL VPN enabled and secondary authentication on any tunnel group must act; the CISA deadline was 1 November

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.6**	STATUS	On CISA's exploited list; due 1 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/cisco-secure-firewall-asa-software-and-cve-2026-76418

The bottom line

> *Organisations running Cisco ASA or FTD with SSL VPN enabled and secondary authentication on any tunnel group must act; the CISA deadline was 1 November 2026. Check tunnel group configuration for secondary-authentication-server-group immediately, including DefaultWEBVPNGroup.*

At a glance

Fact	Detail
Product	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418)
Severity	High: 8.6 (CVSS 3.1)
CISA	On its exploited list since 29 October 2026. Deadline for US federal agencies: 1 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 2 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No source we read names a fixed version
Who looks first	Administrators of Cisco ASA or FTD devices where the SSL remote access VPN login service is reachable from outside, and at least one tunnel group — including the DefaultWEBVPNGroup — has a secondary authentication server group configured.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Cisco Secure Firewall ASA or FTD software?	Nothing to do for this CVE.	Check whether SSL remote access VPN is enabled.
Is SSL remote access VPN enabled on any interface of your ASA or FTD?	Not exposed to this vulnerability.	Check your tunnel group configuration.
Is secondary-authentication-server-group configured in any tunnel group, including DefaultWEBVPNGroup?	Not exposed to this vulnerability.	Check whether the login service is reachable from untrusted networks.

Is the SSL VPN login service reachable from untrusted or internet-facing networks?	Exposure is limited; still apply the update, but not immediately internet-critical.	Act now; the CISA deadline was 1 November 2026.

What it is

An unauthenticated attacker can send a crafted request to the SSL VPN login service and force the firewall to reload, cutting off all traffic through it until it recovers. No account and no user action are needed. The record says the cause is a logic error when secondary authentication is configured on a tunnel group.

Why it matters

The CVSS score of 8.6 reflects no authentication and no user interaction, with the attack crossing a security boundary. The condition that triggers the flaw — secondary authentication on a tunnel group — is a security best practice, so well-secured deployments are more likely to be affected, not less. A successful attack takes the firewall offline. Our reading is that the zero-authentication requirement and network scope make this a priority for any organisation whose remote workforce depends on this VPN, regardless of how narrow the configuration condition appears.

What the vendor's advisory says

We read one page on sec.cloudapps.cisco.com. In short:

- The vendor's advisory (published 28 October 2026, Cisco Bug ID CSCwx26625) explicitly states no workarounds are available. Software updates are the only remediation.
- The advisory's CVSS score is 8.6 (High). The weakness is CWE-690, an unchecked return value to null pointer dereference.

Things people will get wrong

- Removing the group list from the login page removes the risk. The vendor's advisory states that disabling tunnel-group-list does not remove exposure when DefaultWEBVPNGroup has secondary authentication configured. That default group must also be checked.
- Only tunnel groups shown on the login page need checking. The advisory explicitly states the check is not limited to profiles displayed in the group list. All tunnel groups, including hidden ones and the default, must be reviewed.
- The low EPSS score means exploitation is unlikely. CISA has added this to its known-exploited catalogue. The EPSS figure reflects statistical models; CISA's listing reflects observed exploitation in practice, which overrides the probability estimate.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Identify which devices run ASA or FTD

- Compile a list of all Cisco ASA and FTD devices in your estate, noting their software version and whether the SSL VPN service is enabled on any interface.

```
show version
show running-config webvpn
```

Step 2: Check tunnel group configuration for secondary authentication

- On each device with SSL VPN enabled, check every tunnel group including DefaultWEBVPNGroup for secondary-authentication-server-group.
- The advisory says the check applies even when tunnel-group-list is disabled, because DefaultWEBVPNGroup remains active as the default and must be inspected separately.

```
show running-config tunnel-group
```

Step 3: Apply the vendor's software update

- The vendor's advisory states software updates have been released. Check the Fixed Software section of the advisory for the correct release for your ASA or FTD version train.
- There are no workarounds. If patching must be delayed, consider restricting access to the SSL VPN login service to trusted source addresses as a temporary measure.

Step 4: Verify and confirm the fix is in place

- After updating, re-run the configuration checks to confirm no tunnel group retains a vulnerable configuration, and verify the device version reflects the patched release.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits

exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of CVE-2026-76418, a vulnerability in Cisco Secure Firewall ASA and FTD software. An unauthenticated attacker can crash the firewall by sending a crafted request to the SSL VPN login service when secondary authentication is configured on a tunnel group. The CISA remediation deadline was 1 November 2026. Could you please confirm: (1) whether we run any Cisco ASA or FTD devices with SSL VPN enabled; (2) if so, which software version each device is running; and (3) whether secondary authentication is configured on any tunnel group, including DefaultWEBVPNGroup? The vendor's advisory states software updates have been released. Please provide written confirmation of the version running on each affected device and whether the update has been applied or is scheduled, by 8 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected device reloads in the system log correlated in time with SSL VPN connection attempts.
- Malformed or unusual connection requests in the SSL VPN access log immediately before a reload event.
- Reload reason entries in the device's crash or system log pointing to a null pointer dereference in the VPN process.

The weakness behind it

The record classes this as CWE-690 (Unchecked Return Value to NULL Pointer Dereference).

The sources, in their words

CISA's catalogue entry:

> *Cisco Secure Firewall ASA Software and Cisco Secure FTD Software contains an unchecked return value to NULL pointer dereference vulnerability that could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.*

The CVE record, published by Cisco on 28 October 2026:

> *A vulnerability in the Remote Access SSL VPN service of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to logic errors when secondary authentication is configured on a tunnel group. An attacker could exploit this vulnerability by sending a crafted request when connecting to the SSL remote access VPN. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.*

The record lists 142 affected versions or ranges of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software. The first 8 are below; the rest are in the CVE record, so check your version against the whole list.

- 9.16.1
- 9.16.1.28
- 9.16.2
- 9.16.2.3
- 9.16.2.7
- 9.16.2.11
- 9.16.2.13
- 9.16.2.14

The record lists 67 affected versions or ranges of Cisco Secure Firewall Threat Defense (FTD) Software. The first 8 are below; the rest are in the CVE record, so check your version against the whole list.

- 7.0.0
- 7.0.0.1
- 7.0.1
- 7.0.1.1
- 7.0.2
- 7.2.0
- 7.0.2.1
- 7.0.3

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-76418
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-76418
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The provided advisory text does not state specific fixed version numbers for ASA or FTD; the advisory's Fixed Software section must be consulted directly.
- Whether an exploit attempt leaves log entries distinguishable from a routine device reload is not stated in the record.
- Recovery time and behaviour after an exploit-triggered reload is not stated.
- Whether the flaw affects ASA or FTD running as virtual instances is not confirmed in the available source text.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 2 November 2026; the vendor's advisory wins where it differs.

- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-76418: score 8.6, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	None	Nothing can be altered.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
28 October 2026	CVE record published by Cisco.
29 October 2026	CISA added it to its list of exploited vulnerabilities.
1 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
ASA or FTD with SSL VPN enabled, secondary auth on any tunnel group, login page internet-facing	High	Within CISA's window — deadline was 1 November 2026
ASA or FTD with SSL VPN enabled, secondary auth on DefaultWEBVPNGroup even without tunnel-group-list	High	Within CISA's window — deadline was 1 November 2026
ASA or FTD with SSL VPN and secondary auth, reachable only from trusted internal networks	Medium	This week

ASA or FTD with SSL VPN enabled but no secondary authentication configured on any tunnel group	Low	Next patch cycle
ASA or FTD without SSL VPN enabled on any interface	None	None for this CVE

Appendix 4. Definition of done

- Every Cisco Secure Firewall ASA Software and Cisco Secure FTD Software you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-76418: https://www.cve.org/CVERecord?id=CVE-2026-76418
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/c: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75