

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

CISA added CVE-2026-76418 to its exploited list on 29 October 2026; its date is 1 November 2026. What it is, who is affected, and what to do first.

PREPARED BY	NamiQ	DATE	30 October 2026
FACTS AS OF	30 October 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 short version

CISA added Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418) to its list of exploited vulnerabilities on 29 October 2026. That list holds only flaws CISA has evidence are being used in attacks.

Its deadline for US federal agencies is 1 November 2026. Treat it as a date to aim for. It does not bind you.

The base score is 8.6 (CVSS 3.1). EPSS, the estimated chance of exploitation in the next 30 days, is 0.01. Read on 30 October 2026.

Our reading

A remote attacker with no login can send a crafted request to the Remote Access SSL VPN service and make the firewall reload unexpectedly. That cuts VPN service and anything else the device carries. The record blames logic errors when secondary authentication is set on a tunnel group.

Firms running Cisco Secure Firewall ASA or Secure Firewall Threat Defense (FTD) with the SSL remote access VPN switched on, above all where a tunnel group uses secondary authentication.

What happened

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.

That is CISA's description from its catalogue entry.

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

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.

Are you affected?

The record lists 142 affected versions or ranges of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software. The first 8 are:

- 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 rest are in the CVE record (linked under Sources). Check your version against the whole list, not only these.

The record lists 67 affected versions or ranges of Cisco Secure Firewall Threat Defense (FTD) Software. The first 8 are:

- 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

The rest are in the CVE record (linked under Sources). Check your version against the whole list, not only these.

If you run it, find the version number first. If you cannot say what you run, that is the first job, and your IT provider can answer it in minutes.

What to do first

CISA's required action:

Apply mitigations in accordance with vendor instructions.

CISA's date is 1 November 2026. In order:

- List every Cisco ASA and FTD device that offers SSL remote access VPN to staff or suppliers.
- On each one, check whether any tunnel group has secondary authentication configured. The record ties the fault to that setting.
- Compare each device's running software version with Cisco's full affected list. The record names many versions for both products.

- CISA's wording adds that you should stop using the product if no mitigation is available.
- If you cannot do it today, write down who owns it, the new date, and what limits exposure until then, such as restricting the interface to administrator networks.

How to check it is fixed

- The product reports a version outside the affected list. Read it from the product itself, not from an old inventory.
- Save the output or a screenshot with the date, so you can show later when it was done.

If it was exposed before you updated

CISA lists this because attacks have happened. An update closes the hole. It does not tell you whether someone used it first. Look in the product's logs and the web server's logs for the weeks before the update, and for accounts or files you did not create. CISA's required action also points to its forensic triage requirements (BOD 26-04).

- Unexpected device reloads, especially repeated ones, or reboots nobody scheduled.
- VPN users dropped at the moment of a reload.
- Connection attempts to the SSL VPN from unfamiliar addresses shortly before a reload.

The weakness behind it

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

What we could not confirm

- CISA records ransomware use as not recorded. That means not recorded, not that none has happened. No attacker is named in the sources.
- We have not tested this against any environment. This note reports what the sources say and what we would check first.
- Version ranges are as the CVE record state them. The vendor's advisory wins where it differs.
- EPSS and scores move. The figures are as at 30 October 2026.
- The paragraphs headed "Our reading" and the numbered steps 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.
30 October 2026	The facts in this report were read.
1 November 2026	CISA's deadline for US federal agencies.

Appendix 3. 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.
- 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/>
- Reference in the CVE record: sec.cloudapps.cisco.com: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75>