

# CVE-2026-76418

## Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability

CISA KEV since Oct 29, 2026

Actively exploited

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.

|                                                                     |                                              |                                                          |                                                                               |
|---------------------------------------------------------------------|----------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>75</b> / <sub>100</sub><br><b>Urgent</b> priority | <b>CVSS V3.1</b><br><b>8.6</b><br>High · NVD | <b>EPSS</b><br><b>0.006</b><br>47.3rd percentile · FIRST | <b>CISA DEADLINE</b><br><b>Nov 1, 2026</b><br>CISA federal deadline in 2 days |
|---------------------------------------------------------------------|----------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                           |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|-------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild        |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input checked="" type="checkbox"/> <b>KEV recency</b>         | Added to CISA KEV within the last 30 days |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.006 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable             |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 8.6                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                       |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

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.

### Affected and fixed versions

| PACKAGE                                                            | AFFECTED | FIXED IN                | SOURCE |
|--------------------------------------------------------------------|----------|-------------------------|--------|
| Cisco / Secure Firewall ASA Software and Cisco Secure FTD Software | –        | no fixed version listed | NVD    |

### Sources

|                        |                                                                                                                                                                                             |                                                                       |                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/advisories/GHSA-3whv-82g3-5cwX">github.com/advisories/GHSA-3whv-82g3-5cwX</a>                                                                                   | <a href="https://sec.cloudapps.cisco.com">sec.cloudapps.cisco.com</a> | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75">sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75</a>   |
| <b>BOD 26-04</b>       | <a href="https://cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk</a> | <b>Forensics Triage Requirements</b>                                  | <a href="https://cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk</a> |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-76418">nvd.nist.gov/vuln/detail/CVE-2026-76418</a>                                                                                       | <b>CISA KEV</b>                                                       | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                                                     |
| <b>ENISA EUVD</b>      | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-112462">euvd.enisa.europa.eu/vulnerability/EUVD-2026-112462</a>                                                               | <b>Current data</b>                                                   | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-76418">evulnable.com/vulnerability-management/cve/CVE-2026-76418</a>                                                                                                   |



Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.