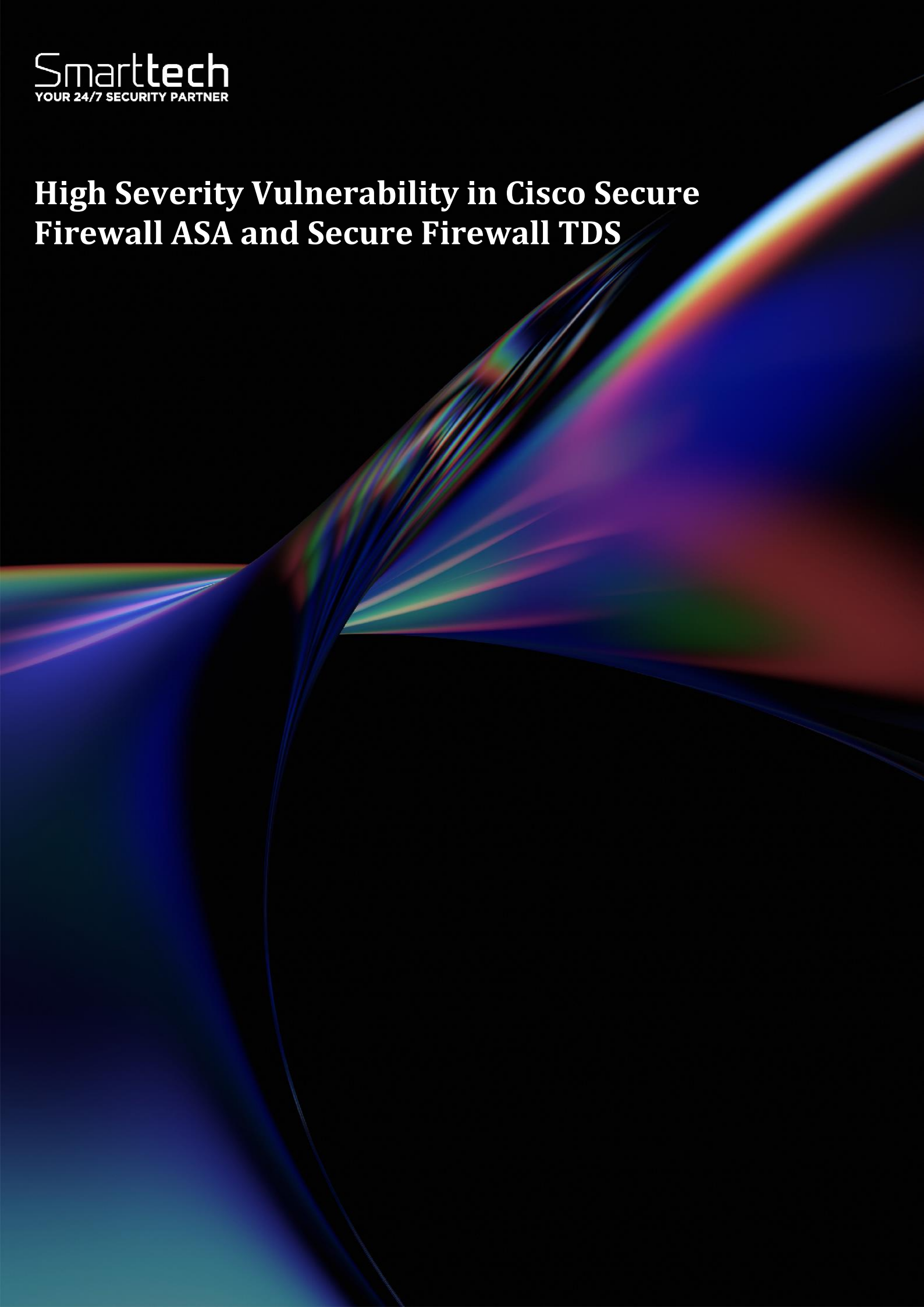
Smarttech
YOUR 24/7 SECURITY PARTNER

# High Severity Vulnerability in Cisco Secure Firewall ASA and Secure Firewall TDS



| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 134 |
| **Authors** | Vlad Dumitrescu <vlad.dumitrescu@smarttech247.com> |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 12th August 2026 |
| **Issue Date** | 11th August 2026 |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview:

A vulnerability in the Remote Access SSL VPN service for 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 insufficient error checking when processing HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the Remote Access SSL VPN service on an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.

## Risk:

**Government**:
- Large and medium government entities: **Critical**
- Small government entities: **Critical**

**Businesses**:
- Large and medium business entities: **Critical**
- Small business entities: **Critical**

## Technical summary

The high-severity flaw, tracked as CVE-2026-20349 (CVSS score: 8.6), is a case of insufficient error checking when processing HTTP requests that could allow an unauthenticated, remote attacker to trigger a denial-of-service (DoS) condition.

### Affected Products

This vulnerability affects Cisco devices if they are running a vulnerable release of Cisco Secure Firewall ASA Software or Cisco Secure FTD Software and have one or more of the vulnerable configurations listed in the following table.

Cisco Secure Firewall ASA and FTD Software Vulnerable Configurations

In the following table, the left column lists Cisco Secure Firewall ASA and Secure FTD Software features that are potentially vulnerable. The right column indicates the basic configuration for the feature from the show running-config CLI command. These features

could enable the SSL listen sockets.

| Cisco Secure Firewall ASA and FTD Software Feature | Possible Vulnerable Configuration |
|---|---|
| IKEv2 Remote Access VPN (with client services)[1] | crypto ikev2 enable <*interface_name*> client-services port <*port_numbers*> |
| SSL VPN[1] | webvpn<br>enable <*interface_name*> |
| Zero Trust Network Access[2] | zero-trust<br>enable |

1. For Cisco Secure FTD Software, remote access VPN features are enabled from Devices > VPN > Remote Access in Cisco Secure Firewall Management Center (FMC) Software or from Remote Access VPN in Cisco Secure Firewall Device Manager (FDM).
2. This feature is available only in Cisco Secure FTD Software.

Cisco has confirmed that this vulnerability does not affect Cisco Secure Firewall Management Center (FMC) Software.

### Cisco Secure Firewall ASA Hot Fixes

Cisco has released the following hot fixes to address this vulnerability. Customers can download the hot fixes from the Software Center on Cisco.com.

| Cisco Secure Firewall ASA Software Release | Hot Fix Name |
|---|---|
| 9.16[1] | 89.16.4.50 |
| 9.18[1] | 89.18.4.50 |
| 9.20 | 9.20.4.235 |
| 9.22 | 9.22.3.191 |
| 9.23 | 9.23.1.211 |
| 9.24 | 9.24.1.221 |

1. When installing a hot fix that starts with 89, install ASDM Release 7.24.1.374 because previous releases of ASDM do not recognize this ASA Software release numbering format.

### Cisco Secure FTD Hot Fixes

| Cisco Secure FTD Software Release | Hot Fix Name |
|---|---|
| 7.0 | Cisco_FTD_Hotfix_GC-7.0.9.1-1.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_GC-7.0.9.1-1.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_GC-7.0.9.1-1.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_GC-7.0.9.1-1.sh.REL.tar |
| 7.2 | Cisco_FTD_Hotfix_HM-7.2.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_HM-7.2.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_HM-7.2.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_HM-7.2.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_HM-7.2.11.1-2.sh.REL.tar |
| 7.4 | Cisco_FTD_Hotfix_HK-7.4.7.1-1.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_HK-7.4.7.1-1.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_HK-7.4.7.1-1.sh.REL.tar |

| | |
|---|---|
| | Cisco_FTD_SSP_FP3K_Hotfix_HK-7.4.7.1-1.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_HK-7.4.7.1-1.sh.REL.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_HK-7.4.7.1-1.sh.REL.tar |
| 7.6 | Cisco_FTD_Hotfix_DD-7.6.4.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_DD-7.6.4.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_DD-7.6.4.1-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_DD-7.6.4.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_DD-7.6.4.1-2.sh.REL.tar |
| 7.7 | Cisco_FTD_Hotfix_AN-7.7.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_AN-7.7.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_AN-7.7.11.1-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_AN-7.7.11.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_1200_Hotfix_AN-7.7.11.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_AN-7.7.11.1-2.sh.REL.tar |
| 10.0 | Cisco_FTD_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_200_Hotfix_R-10.0.0.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_1200_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_S-10.0.0.1-2.sh.REL.tar<br>Cisco_Secure_FW_TD_6100_Hotfix_S-10.0.0.1-2.sh.REL.tar |

Note: For instructions on upgrading a Cisco Secure FTD device, see the appropriate Cisco Secure FMC upgrade guide.

**Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software**

To help customers determine their exposure to vulnerabilities in Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described in each advisory ("First Fixed"). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities that are described in all the advisories that the Software Checker identifies ("Combined First Fixed").

To use the tool, go to the Cisco Software Checker page and follow the instructions.

**Exploitation and Public Announcements**

In August 2026, the Cisco Product Security Incident Response Team (PSIRT) became aware of active exploitation of this vulnerability. Cisco strongly recommends that customers upgrade to a fixed software release to remediate this vulnerability.

## Recommendations

The **Smarttech247** team recommends the following actions**:**

- Apply the appropriate patches or appropriate mitigations provided by Cisco to vulnerable systems immediately after appropriate testing.

- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Ensure that endpoint security and perimeter security products are updated

## References

Cisco:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF#fs
Bleeping Computer:
https://www.bleepingcomputer.com/news/security/cisco-warns-of-asa-and-ftd-vpn-flaw-exploited-to-crash-devices/

## CVEs

CVE-2026-20349


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com