GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

12 August 2026

Advisory 184: CVE-2026-20349_Cisco Secure Firewall ASA and FTD Remote Access SSL VPN Denial of Service Vulnerability

Release Date: 11th August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-20349 is a high-severity denial of service 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. It carries a CVSS Base Score of 8.6 and is due to insufficient error checking when processing HTTP requests.
An unauthenticated, remote attacker can exploit this vulnerability by sending a crafted HTTP request to the Remote Access SSL VPN service on an affected device, causing the device to reload unexpectedly and resulting in a denial of service (DoS) condition.

What are the systems affected?

Affected systems include Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software with Remote Access SSL VPN, IKEv2 Remote Access VPN with client services, or Zero Trust Network Access enabled.

Cisco Secure Firewall ASA Software – (Affected)
Cisco Secure Firewall Threat Defense (FTD) Software – (Affected)
IKEv2 Remote Access VPN (with client services) – (Vulnerable configuration)
SSL VPN (webvpn enabled) – (Vulnerable configuration)
Zero Trust Network Access (FTD only) – (Vulnerable configuration)
Cisco Secure Firewall Management Center (FMC) Software – (Confirmed Not Vulnerable)

Any organisation running internet-facing ASA or FTD Remote Access VPN services is at risk, given confirmed active exploitation.

What does this mean?

This flaw in the Remote Access SSL VPN service stems from insufficient error checking when the device parses incoming HTTP requests. No authentication and no user interaction are required, and the attacker needs only network reachability to the VPN service to trigger it.

Step 1 - Exposure
A device is reachable if it has one or more of the following features enabled and listening on an interface:

- IKEv2 Remote Access VPN with client services (crypto ikev2 enable <interface> client-services)
- SSL VPN (webvpn enable <interface>)
- Zero Trust Network Access (zero-trust enable) - FTD only

Step 2 - Exploitation
The attacker sends a crafted HTTP request to the Remote Access SSL VPN service on the affected device. Insufficient error checking during processing of the request triggers the underlying fault condition (CWE-244).

Step 3 - Device Reload
The fault condition causes the affected device to reload unexpectedly, dropping active VPN sessions and preventing new Remote Access SSL VPN connections until the device has fully recovered.

Step 4 - Repeated Exploitation
Because the request requires no authentication, an attacker can repeat it after each reload to keep the Remote Access VPN service unavailable indefinitely, disrupting remote connectivity for legitimate users and administrators.

Mitigation process

CERTVU recommends the following:

Primary - Apply Cisco Hot Fixes Immediately

Cisco has released hot fixes for affected ASA releases (9.16, 9.18, 9.20, 9.22, 9.23, 9.24) and affected FTD releases (7.0, 7.2, 7.4, 7.6, 7.7, 10.0). There are no workarounds. Given confirmed active exploitation and the 14 August 2026 CISA KEV remediation deadline, administrators should use the Cisco Software Checker to confirm the correct hot fix for their release and apply it as an

emergency, out-of-band change rather than waiting for a scheduled maintenance window. Devices with IKEv2 Remote Access VPN, SSL VPN, or Zero Trust Network Access enabled should be prioritised.

Cisco Security Advisory: cisco-sa-asaftd-vpn-dos-dzv4mQFF

Secondary - Review VPN Exposure

Confirm whether Remote Access SSL VPN, IKEv2 Remote Access VPN with client services, or Zero Trust Network Access is enabled on internet-facing ASA/FTD devices, and monitor for unexpected device reloads consistent with this DoS condition until the hot fix is applied.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-20349
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF

.