Security Advisory 2025-036

Critical Vulnerabilities in Cisco ASA and FTD

2025-09-26 — v1.1

TLP:CLEAR

History:

- *26/09/2025 — v1.0 – Initial publication*
- *26/09/2025 — v1.1 – Added information about vulnerable configuration*

Summary

On September 25, 2025, Cisco released several security advisories addressing 3 vulnerabilities, 2 of which are critical [1,2,3,4]. Cisco warns that some of those vulnerabilities are exploited in the wild and assesses with high confidence that this new activity is related to the same threat actor as the ArcaneDoor attack campaign that Cisco reported in early 2024 [4].

It is recommended running compromise assessment on Internet facing vulnerable devices, and update as soon as possible.

Technical Details

The vulnerability **CVE-2025-20333**, with a CVSS score of 9.9, is due to improper validation of user-supplied input in HTTP(S) requests. An attacker with valid VPN user credentials could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as root, possibly resulting in the complete compromise of the affected device. This vulnerability affects the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software [1]. The Cisco PSIRT is **aware of attempted exploitation** of this vulnerability.

The vulnerability **CVE-2025-20363**, with a CVSS score of 9.0, is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web service on an affected device after obtaining additional information about the system, overcoming exploit mitigations, or both. A successful exploit could allow the attacker to execute arbitrary code as root, which may lead to the complete compromise of the affected device. This vulnerability affects the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software [2]. The Cisco PSIRT is **not aware of any public announcements or malicious use** of this vulnerability.

The vulnerability **CVE-2025-20362**, with a CVSS score of 6.5, is due to improper validation of user-supplied input in HTTP(S) requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on a device. A successful exploit could allow the attacker to access a restricted URL without authentication. This vulnerability affects the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software [3]. The Cisco PSIRT is aware of **attempted exploitation of this vulnerability**.

Affected Products

[UPDATED] The following versions of Cisco ASA and FTD are affected by all 3 vulnerabilities (refer to the **[NEW]** Vulnerable configurations subsection for more information):

- Cisco ASA:
  - version 9.16 before 9.16.4.85
  - version 9.17
  - version 9.18 before 9.18.4.67
  - version 9.19
  - version 9.20 before 9.20.4.10
  - version 9.22 before 9.22.2.14
  - version 9.23 before 9.23.1.19
- Cisco FTD:
  - version 7.0 before 7.0.8.1
  - version 7.1
  - version 7.2 before 7.2.10.2
  - version 7.3
  - version 7.4 before 7.4.2.4
  - version 7.6 before 7.6.2.1
  - version 7.7 before 7.7.10.1

The IOS, IOS XE, and IOS XR Software are also vulnerable to **CVE-2025-20363** [2] (refer to the **[NEW]** Vulnerable configurations subsection for more information).

Customers should use the Cisco Software Checker to determine the appropriate patched release for their specific software train.

[NEW] Vulnerable Configurations

CVE-2025-20333 and CVE-2025-20362

Please refer to the Cisco's advisory for CVE-2025-20333 and the Cisco's advisory for CVE-2025-20362 for more detailed information on how to check device configuration.

Cisco Secure Firewall ASA Software Vulnerable Configurations

Cisco lists the following Cisco Secure Firewall ASA Software features as potentially vulnerable:

- AnyConnect IKEv2 Remote Access (with client services)
- Mobile User Security (MUS)
- SSL VPN

Cisco Secure Firewall FTD Software Vulnerable Configurations

Cisco lists the following Cisco Secure Firewall FTP Software features as potentially vulnerable:

- AnyConnect IKEv2 Remote Access (with client services)
- AnyConnect SSL VPN

CVE-2025-20363

Please refer to Cisco's advisory for more detailed information on how to check device configuration.

Cisco Secure Firewall ASA Software Vulnerable Configurations

Cisco lists the following Cisco Secure Firewall ASA Software features as potentially vulnerable:

- Mobile User Security (MUS)
- SSL VPN

Cisco Secure Firewall FTD Software Vulnerable Configurations

Cisco lists the following Cisco Secure Firewall FTP Software features as potentially vulnerable:

- AnyConnect SSL VPN

Cisco IOS and IOS XE Software Vulnerable Configurations

Cisco lists the following Cisco Secure Firewall FTP Software features as potentially vulnerable:

- Remote Access SSL VPN

IOS XR Software

Cisco lists the following Cisco Secure Firewall FTP Software features and configuration as potentially vulnerable:

- 32-bit version
- Running on Cisco ASR 9001 Routers
- HTTP server enabled

Recommendations

It is recommended running compromise assessment on Internet facing vulnerable devices, and update as soon as possible.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW

[4] https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks