Two critical bugs in Cisco ASA and FTD: score 9.9 and risk of remote code

Data: 2025-09-25 17:31:02

Autor: Inteligência Against Invaders

Redazione RHC:**25 September 2025 19:29**

Cisco has disclosed two critical vulnerabilities affecting its **Secure Firewall Adaptive Security Appliance (ASA)** and **Secure Firewall Threat Defense (FTD)** firewalls, as well as other networking products. Both flaws allow arbitrary code execution and could lead to the complete compromise of affected devices.

CVE-2025-20363 – Code Execution via Web Services

The first vulnerability, identified as CVE-2025-20363 and with **CVSS score 9.0 (critical)** , affects the web services of:

- Cisco Secure Firewall ASA Software
- Cisco Secure Firewall FTD Software
- Cisco IOS Software
- Cisco IOS XE Software
- Cisco IOS XR Software

Cisco Secure Firewall ASA Software Feature	Possible Vulnerable Configuration
AnyConnect IKEv2 Remote Access (with client services)	crypto ikev2 enable interface name > client-services port port_numbers >
Mobile User Security (MUS)	webvpn mus password mus server enable port_number > mus IPv4_address > IPv4_mask > interface_name >
SSL VPN	webvpn enable

For ASA and FTD firewalls, the flaw can be exploited by an **unauthenticated** remote attacker. For IOS, IOS XE, and IOS XR platforms, low-privilege credentials are required.

The root of the problem lies in improper input handling in HTTP requests. An attacker can send manipulated packets to exposed web services from a vulnerable device, allowing them to execute arbitrary code with **root** privileges. Such a compromise could result in complete system control.

CVE-2025-20333 – VPN Server Vulnerability

The second flaw, classified as CVE-2025-20333 , has an even higher **CVSS score of 9.9 (critical)** . It only affects **ASA** and **FTD** firewalls when the web VPN server is active.

The flaw, again caused by a failure to validate input in **HTTP(S)** requests, can be exploited by a remote attacker with valid VPN credentials. The outcome of a successful attack is identical to the previous one: arbitrary code execution as root and potential complete compromise of the device.

Cisco Secure Firewall ASA Software Feature Mobile User Security (MUS)	Possible Vulnerable Configuration webvpn mus password mus server enable port Port_number > mus IPv4_address > IPv4_mask > interface_name >
SSL VPN	webvpn enable

Cisco Advisory and Recommendations

Cisco has published an **official security advisory** (ID: *cisco-sa-asaftd-webvpn-z5xP8EUB* , released **September 25, 2025**) regarding the CVE-2025-20333 vulnerability.
Among the main details:

- **Severity:** Critical
- **CVSS Score:** 9.9 (CVSS v3.1 / AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
- **Cisco Bug ID:** CSCwq79831
- **Workaround:** None available
- **Advisory Version:** 1.0, Final

Devices are vulnerable if they are running an affected release of the ASA or FTD software and have VPN or SSL configurations enabled (for example, AnyConnect IKEv2, Mobile User Security, or SSL VPN).

Cisco specifies that:

- No effective workarounds have been identified.
- Software updates are available that fix the flaw.
- It is strongly recommended that you update to a fixed release immediately.

Exploit and impact

The **Cisco Product Security Incident Response Team (PSIRT)** has reported that it is already aware of attempts to actively exploit the VPN server vulnerability. For this reason, the company reiterates the urgency of applying updates.

The vulnerability was discovered during the resolution of a Cisco TAC technical support case, with input from several security agencies, including:

- **Australian Signals Directorate – Australian Cyber Security Centre**
- **Canadian Center for Cyber Security**

- **UK National Cyber Security Center (NCSC)**
- **US Cybersecurity & Infrastructure Security Agency (CISA)**

Support tools

To check if a specific device is vulnerable, Cisco provides the **Cisco Software Checker** , which allows you to:

- Identify advisories that impact a specific release.
- Locate the first software release that fixes the problem.
- Determine the release that addresses all known vulnerabilities.

Conclusions

The CVE-2025-20363 and CVE-2025-20333 vulnerabilities pose significant risks to corporate network infrastructure. The ability to execute arbitrary code as root makes affected devices particularly vulnerable to full compromise.

Cisco therefore invites customers to update their ASA and FTD firewalls without delay, following the instructions in the official advisory available at the link:

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli