Cisco warns customer of ASA firewall zero-days exploited in attacks – Info

Data: 2025-09-26 01:41:04

Autor: Inteligência Against Invaders

infosecbulletin

3 minutes ago
Alert, Vulnerabilities

Cisco warned customers to patch two zero-day vulnerabilities that are actively being exploited in attacks and impact the company's firewall software.

The first one (CVE-2025-20333) allows authenticated, remote attackers to execute arbitrary code on devices running vulnerable Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) software, while the second (CVE-2025-20362) enables remote attackers to access restricted URL endpoints without authentication.

"The Cisco Product Security Incident Response Team (PSIRT) is ***aware*** of attempted exploitation of this vulnerability," the company warned in security advisories regarding the two zero-day flaws.

"Cisco continues to strongly recommend that customers upgrade to a fixed software release to remediate this vulnerability."

The company also thanked the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the UK National Cyber Security Centre (NCSC), and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) for their assistance in investigating the CVE-2025-20333 and CVE-2025-20362 ***zero-day*** attacks.

While it didn't directly link it to these attacks, Cisco patched a third critical vulnerability (CVE-2025-20363) in firewall and Cisco IOS software that can let unauthenticated threat actors to execute arbitrary code remotely on unpatched devices.

Today's security patches come weeks after cybersecurity company GreyNoise detected two large-scale campaigns in late August, with up to 25,000 unique IP addresses targeting ASA login portals and Cisco IOS Telnet/SSH services exposed online.

GreyNoise has previously reported that such reconnaissance activity precedes the disclosure of new security vulnerabilities impacting the probed products in 80% of cases.

At the time, BleepingComputer contacted Cisco for comment on the observed malicious activity, but we have yet to receive a reply.

On Wednesday, Cisco released another set of security patches for a high-severity zero-day vulnerability in Cisco IOS and IOS XE software, which is also being exploited in the wild.

In May, the company also warned of a maximum severity IOS XE flaw impacting Wireless LAN Controllers, which enables unauthenticated attackers to take over devices remotely.