CISA orders agencies to patch Cisco flaws exploited in zero-day attacks -

Data: 2025-09-25 20:07:35

Autor: Inteligência Against Invaders

CISA has issued a new emergency directive ordering U.S. federal agencies to secure their Cisco

firewall devices against two flaws that have been exploited in zero-day attacks.

Emergency Directive 25-03 was issued to Federal Civilian Executive Branch (FCEB) agencies on September 25 and requires them to patch CVE-2025-20333 and CVE-2025-20362 vulnerabilities in Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) software.

“The campaign is widespread and involves exploiting zero-day vulnerabilities to gain unauthenticated remote code execution on ASAs, as well as manipulating read-only memory (ROM) to persist through reboot and system upgrade. This activity presents a significant risk to victim networks,” CISA warned today.

“CISA is directing agencies to account for all Cisco ASA and Firepower devices, collect forensics and assess compromise via CISA-provided procedures and tools, disconnect end-of-support devices, and upgrade devices that will remain in service.”

The U.S. cybersecurity agency now requires all FCEB agencies to identify all Cisco ASA and Firepower appliances on their networks, disconnect all compromised devices from the network, and patch those that show no signs of malicious activity by 12 PM EDT on September 26.

Additionally, CISA ordered that agencies must permanently disconnect ASA devices that are reaching the end of support by September 30 from their networks.

Exploitation linked to 2024 ArcaneDoorcampaign

Cisco has released security updates to address the two security flaws earlier today, saying that CVE-2025-20333 can allow authenticated attackers to remotely gain code execution on vulnerable devices, while CVE-2025-20362 enables remote threat actors to access restricted URL endpoints without authentication.

When chained, the two vulnerabilities can enable unauthenticated attackers to gain full control of unpatched devicesremotely.

“Attackers were observed to have exploited multiple zero-day vulnerabilities and employed advanced evasion techniques such as disabling logging, intercepting CLI commands, and intentionally crashing devices to prevent diagnostic analysis,” Cisco said today, adding that the attacks targeted 5500-X Series devices with VPN web services enabled.

“During our forensic analysis of confirmed compromised devices, in some cases, Cisco has observed the threat actor modifying ROMMON to allow for persistence across reboots and software upgrades."

CISA and Cisco linked these ongoing attacks to the ArcaneDoor campaign, which exploited two other ASA and FTD zero-days (CVE-2024-20353 and CVE-2024-20359) to breach government networks worldwide since November 2023.

Cisco became aware of the ArcaneDoor attacks in early January 2024 and discovered evidence that the UAT4356 threat group behind the campaign (tracked as STORM-1849 by Microsoft) had tested and developed exploits for the two zero-days since at least July 2023.

In the attacks, the hackers deployed previously unknown Line Dancer in-memory shellcode loader and Line Runnerbackdoor malware to maintain persistence on compromised Cisco devices.

On Friday,Cisco patched a third critical vulnerability (CVE-2025-20363) in its firewall and Cisco IOS software, which can let unauthenticated threat actors to execute arbitrary code remotely on unpatched devices.

However,the company didn't directly link it to these attacks in today's advisory, saying that its Product Security Incident Response Team"is not aware of any public announcements or malicious use of the vulnerability."

[IMAGEM REMOVIDA]