50K Cisco firewalls vulnerable to actively exploited flaws - InfoSecBulletin

Data: 2025-09-30 19:31:56

Autor: Inteligência Against Invaders

infosecbulletin

4 minutes ago
Alert, Cyber Attack, Vulnerabilities

50k Cisco ASA and FTD devices on the internet are at ***risk*** due to two vulnerabilities being exploited by hackers. Flaws CVE-2025-20333 and CVE-2025-20362 allow remote code execution and access to restricted VPN URLs without authentication.

On September 25, Cisco warned that the issues were actively exploited in attacks that started before patches were available to customers. There are no solutions for either flaw, but temporary measures could involve limiting VPN web interface access and enhancing logging and monitoring for unusual VPN logins and requests.

The Shadowserver Foundation ***reported*** that over 48,800 exposed ASA and FTD instances are still vulnerable to CVE-2025-20333 and CVE-2025-20362.

Most IPs are from the United States, followed by the United Kingdom, Japan, Germany, Russia, Canada, and Denmark.

As of September 29, these figures show a failure to address ongoing exploitation and earlier warnings.

Greynoise warned on September 4 about suspicious scans targeting Cisco ASA devices that began in late August. These scans often indicate potential undocumented flaws in 80% of cases.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an urgent directive, allowing 24 hours for all Federal Civilian Executive Branch (FCEB) agencies to find and upgrade compromised Cisco ASA and FTD instances on their networks.

CISA also advised that ASA devices reaching their end of support (EoS) should be disconnected from federal organization networks by today (the end of the month).