U.S. CISA adds CISCO Secure Firewall ASA and Secure FTD flaws to its Kr

Data: 2025-09-25 20:02:57

Autor: Inteligência Against Invaders

U.S. CISA adds CISCO Secure Firewall ASA and Secure FTD flaws to its Known Exploited Vulnerabilities catalog

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds CISCO Secure Firewall ASA and Secure FTD flaws to its Known Exploited Vulnerabilities catalog.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA)added CISCO Secure Firewall ASA and Secure FTD flaws to its Known Exploited Vulnerabilities (KEV) catalog.

CISA urges Federal Agencies to identify and mitigate potential compromise of Cisco devices.

“CISA is aware of an ongoing exploitation campaign by an advanced threat actor targeting Cisco Adaptive Security Appliances (ASA). 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.” states CISA’s emergency directive. “This activity presents a significant risk to victim networks. Cisco assesses that this campaign is connected to theArcaneDooractivity identified in early 2024 and that this threat actor has demonstrated a capability to successfully modify ASA ROM at least as early as 2024. These zero-day vulnerabilities in the Cisco ASA platform are also present in specific versions of Cisco Firepower.“

Below are the descriptions for these flaws:

- CVE-2025-20362 – Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability:*Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Software VPN Web Server contain a missing authorization vulnerability. This vulnerability could be chained with CVE-2025-20333.*
- CVE-2025-20333 – Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability:*Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Software VPN Web Server contain a buffer overflow vulnerability that allows for remote code execution. This vulnerability could be chained with CVE-2025-20362.*

CISA’s Emergency Directive orders agencies to identify all Cisco ASA and Firepower devices, follow core dump analysis steps, and submit results by Sept 26, 2025. If compromised, devices must be isolated and impacted agencies must report the incidents. Agencies must update supported devices within strict deadlines, retire unsupported models, and report full inventories with actions taken by Oct

2, 2025.

According toBinding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB agencies have to address the identified vulnerabilities by the due date to protect their networks against attacks exploiting the flaws in the catalog.

Experts also recommend that private organizations review theCatalogand address the vulnerabilities in their infrastructure.

CISA orders federal agencies to fix the vulnerabilities bySeptember 26, 2025.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,cisa)