# Global attacks on Cisco devices: Cyber agencies warn of ongoing crisis -

Data: 2025-09-29 09:13:49

Autor: Inteligência Against Invaders

Redazione RHC**:29 September 2025 10:40**

Major agencies around the world have raised the alarm about a critical threat to network infrastructure: *vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Firepower devices have been targeted by a flurry of attacks* . The alert follows the issuance of Emergency Directive 25-03 by the U.S. **Cybersecurity and Infrastructure Security Agency (CISA)** , requiring all *federal civilian agencies to urgently review and secure their devices to stop a large-scale attack campaign.*

The incident involved the exploitation of several previously unknown vulnerabilities in Cisco systems, allowing unauthorized remote execution of arbitrary code and **even ROM modification to maintain control across reboots and updates.** Both *ASA and Firepower Threat Defense were affected.*

Cisco itself, as reported in the previous article, links the attack to the **ArcaneDoor** campaign, first registered in 2024. While some modern Firepower protections have a Secure Boot mechanism that can detect tampering, a significant number of ASAs remain completely vulnerable.

The situation has resonated well beyond the United States. The French national cybersecurity agency, CERT-FR, published bulletin **CERTFR-2025-ALE-013** , confirming that vulnerabilities CVE-2025-20333 and CVE-2025-20362 are being exploited in various versions of ASA and FTD.

The Australian Cyber Security Centre (ACSC) has recommended that ASA 5500-X owners disable IKEv2 and SSL VPN until patches are available.

The Canadian Cyber Security Centre has warned of the *global spread of sophisticated malware, particularly dangerous for unsupported devices.*

Directive 25-03 details the U.S. agencies' actions. By the end of September, organizations **must submit memory dumps of all publicly accessible ASAs to CISA,** deactivate and register any compromised devices, update all software, and *begin decommissioning the equipment, with support expiring on September 30, 2025.*

For models scheduled for end of support in August 2026, **all updates must be installed within 48 hours of release.** All entities are required to *provide CISA with a full progress report and actionable actions by October 2, 2025.*

These requirements apply not only to equipment located directly at federal agencies, *but also to third-party service and cloud infrastructure, including FedRAMP providers* . Agencies remain responsible for compliance across all environments. For those lacking the necessary technical resources, **CISA**

**has offered specialized assistance.**

Subsequently, by February 1, 2026, a report on the directive’s implementation will be submitted to the U.S. Department of Homeland Security, the *National Director of Cyber Policy, the Office of the Bureau of Investigation (OMB)* , and *the Office of the Federal CISO.* Private and foreign companies are also strongly advised to follow the same data collection and *compromise search process to identify potential signs of exploitation.*

Therefore, the entire Cisco ASA ecosystem is at risk, including legacy models that are not receiving updates.

International warnings emphasize *that this is a large-scale global attack, capable of disabling critical systems if immediate action is not taken.*

**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