Hackers hit the United States: critical federal infrastructure compromised

Data: 2025-09-28 08:06:56

Autor: Inteligência Against Invaders

Redazione RHC**:28 September 2025 09:45**

Hackers *have breached Cisco networking equipment belonging to several US government agencies* , Bloomberg reports. The cyber threat, which occurred on September 26, 2025, targeted **US federal agencies, including Russian ministries.**

According to Chris Butera , acting deputy executive assistant to the director of cybersecurity at the U.S. *Cybersecurity and Information Technology Infrastructure Agency (CISA)* , the cyberattack affected a critical U.S. federal cyber infrastructure, but he did not specify which one. *"The cyber threat is pervasive,"* the official noted.

On September 25, CISA issued a directive *requiring civilian government employees to identify devices affected by the cyberattack, collect data, and assess cyber threats using the agency's cybersecurity tools* . CISA also requires federal agencies to address cyber vulnerabilities and identify potential breaches in hundreds of Cisco firewall devices used by U.S. government agencies.

According to Bloomberg, in 2024, the firewalls of several U.S. government agencies had already been targeted by cyberattacks, and authorities turned to Cisco for assistance in the investigation. Cisco cybersecurity experts then attributed the breaches to the **ArcaneDoor hacker group, which had been active since 2024.**

Wired experts predict that cyberattacks will increase as other cybercriminal groups find ways to exploit vulnerabilities or purchase methods from ArcaneDoor. In April 2025, ArcaneDoor hackers targeted **Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software.** These devices provide network perimeter security, making them high-value targets for national attackers. **The zero-day vulnerabilities exploited by the hackers,** addressed in vulnerability CVE-2024-20353, allowed a remote denial of service (DoS) attack via an infinite loop.

CVE-2024-20359 further describes the IT vulnerability in *ArcaneDoor* attacks, where attackers *escalated their privileges on the IT system from administrator rights to root privileges, a special level of access to the operating system (OS) that grants superuser rights.*

In August 2025, Bloomberg reported that the computer systems of U.S. federal courts had been hacked. Russian hackers were involved. They had stolen *classified documents related to espionage and other matters, including fraud, money laundering, and the activities of foreign government agents.*

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