AL2025_46 Cisco ASA and FTD Zero-Day Vulnerabilities Actively Exploited in State-Sponsored Attacks (October 02nd , 2025)

Description

Cisco has released emergency security patches for three critical zero-day vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) software, two of which are being actively exploited in the wild by an advanced threat actor linked to the ArcaneDoor campaign. The vulnerabilities **CVE-2025-20333**, **CVE-2025-20362**, and **CVE-2025-20363** allow attackers to execute arbitrary code, bypass authentication, and implant persistent malware on affected devices.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) have issued Emergency Directive 25-03, mandating immediate mitigation for federal agencies due to the significant risk posed by this campaign. The threat actor, identified as UAT4356 (also known as Storm-1849), has demonstrated sophisticated capabilities including ROM manipulation to maintain persistence even after device reboots and system upgrades.

Attack Details

The campaign exploits multiple high-severity vulnerabilities to gain and maintain control of targeted network devices: **CVE-2025-20333 (CVSS 9.9)** is a critical remote code execution flaw that lets an authenticated remote attacker with valid VPN credentials execute arbitrary code as root via crafted HTTP requests to the VPN web server, while **CVE-2025-20362 (CVSS 6.5)** is an authentication-bypass flaw enabling unauthenticated attackers to reach restricted URL endpoints with specially crafted requests. In addition, **CVE-2025-20363 (CVSS 9.0)** represents a critical unauthenticated remote code execution weakness in firewall and Cisco IOS software that, though not yet observed in the wild, is assessed as high risk for imminent exploitation. Attackers have been chaining **CVE-2025-20333** and **CVE-2025-20362** to circumvent authentication and achieve full control over vulnerable devices, targeting government networks worldwide for data exfiltration. The threat actor uses advanced evasion techniques (disabling logging, intercepting CLI commands, and deliberately crashing devices to frustrate forensic analysis) and has deployed persistent malware capable of surviving reboots by modifying device ROM a persistence technique first seen in the ArcaneDoor campaign in early 2024. Affected hardware includes Cisco ASA 5500-X series models (5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) and certain Cisco Firepower appliance versions.

Remediation

- Immediately Upgrade to Fixed Releases: Apply Cisco's security patches for your specific ASA or FTD software version. Refer to Cisco's security advisories for detailed fixed release information.
- Federal Agencies - Emergency Compliance: CISA mandates that federal civilian executive branch agencies must disconnect end-of-support devices and upgrade vulnerable devices by 11:59 PM EST on September 26, 2025.

- Verify Device Status: Use Cisco's Software Checker or contact Cisco TAC to determine if your devices are affected and which fixed release to apply.
- Temporary Mitigation (If Patching Not Immediately Possible): Consider disabling SSL/TLS-based VPN web services on affected devices, though this may impact VPN functionality. Review Cisco's advisory for detailed mitigation guidance.
- Implement Detection Measures: Use Cisco's Detection Guide for identifying potential compromises. Review device logs for suspicious activity, unauthorized access attempts, or unexpected device behavior.
- Check for Compromise: If your devices match the vulnerable models, open a Cisco TAC case for forensic analysis to determine if there has been malicious activity.
- Upgrade End-of-Life Devices: Many affected ASA 5500-X Series models are reaching end of support (September 30, 2025, for some models). Plan to upgrade to supported hardware platforms.
- Network Segmentation: Isolate critical firewall devices and restrict administrative access to trusted networks only.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Cisco. (2025, September 25). Continued Attacks against Cisco Firewalls by the Threat Actor behind ArcaneDoor. Retrieved from Cisco Security. https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

- Gatlan, S. (2025, September 25). Cisco warns of ASA firewall zero-days exploited in attacks. Retrieved from Bleeping Computer. https://www.bleepingcomputer.com/news/security/cisco-warns-of-asa-firewall-zero-days-exploited-in-attacks/