

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

Active Zero-Day Exploitation on Cisco ASA and FTD Devices

Date of Publication

September 29, 2025

Admiralty Code

A1










TA Number

TA2025300

Summary

First Seen: August 2025
Affected Product: Cisco ASA and FTD
Threat Actor: UAT4356 (aka Storm-1849)
Malware: RayInitiator bootkit, Line Viper loader
Impact: Cisco ASA and FTD devices are under active attack via zero-day vulnerabilities CVE-2025-20333, CVE-2025-20362, and CVE-2025-20363, which together allow unauthenticated remote root access. CVE-2025-20333 is a VPN web server buffer overflow enabling RCE as root, while CVE-2025-20362 bypasses authentication to expose restricted endpoints. Attackers, linked to the state-sponsored UAT4356/Storm-1849 group, leverage these flaws to install persistent malware like RayInitiator and LINE VIPER, manipulating firmware and ROMMON to survive reboots. Exploitation includes anti-forensic measures such as log tampering and device crashes, making detection and remediation extremely challenging.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-20333	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway			
CVE-2025-20362	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	Citrix NetScaler ADC and NetScaler Gateway			
CVE-2025-20363	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Unauthorized Access Vulnerability	Citrix NetScaler ADC and NetScaler Gateway			

Vulnerability Details

#1

Cisco disclosed two high-impact vulnerabilities in its Secure Firewall Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software CVE-2025-20333, CVE-2025-20362, and CVE-2025-20363. CVE-2025-20333 is a buffer overflow in the VPN web server component that allows an attacker with valid credentials to achieve remote code execution (RCE) as root, resulting in full device compromise.

#2

CVE-2025-20362 is an unauthenticated authorization bypass that exposes restricted VPN endpoints without requiring login. While each flaw is dangerous on its own, when chained together, these vulnerabilities could allow an unauthenticated, remote attacker to gain full control of an affected device. Exploitation has already been observed in the wild, with campaigns targeting exposed ASA/FTD devices. Cisco and CISA confirm that attackers are chaining CVE-2025-20362 with CVE-2025-20333 to bypass authentication requirements and execute arbitrary code remotely.

#3

Both vulnerabilities are confirmed to be under active exploitation by a sophisticated, state-sponsored actor (UAT4356, also known as Storm-1849, it's previously linked to a sophisticated operational cluster called [ArcaneDoor campaign](#)). The observable outcome of a successful exploit chain is full, persistent network compromise. Attackers leverage the root-level RCE to install advanced, evasive malware, notably the RayInitiator bootkit and the LINE VIPER user-mode loader.

#4

This persistence is achieved by manipulating the firewall's firmware and ROM Monitor (ROMMON), allowing the malicious payload to survive system reboots and even software upgrades. Devices, particularly the older ASA 5500-X series lacking modern secure boot features, are primary targets. The exploitation also includes advanced anti-forensic measures, such as disabling logs and crashing the device, making detection and incident response extremely difficult.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-20333	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*	CWE-120
CVE-2025-20362			CWE-862
CVE-2025-20363			CWE-122

Recommendations



Apply Patches and Restrict Exposure: Cisco has released fixed ASA/FTD software versions addressing CVE-2025-20333, CVE-2025-20362, and CVE-2025-20363. Upgrade devices to the recommended builds without delay. Until patching is complete, restrict external access to VPN/web interfaces using ACLs, IP allow-lists, or temporary disablement of remote access features to reduce the attack surface.



Monitor for Adversary Anti-Forensic Activity: Attackers behind this campaign actively suppress syslog messages (302013, 302014, 609002, 710005) and disable the “checkheaps” routine to evade detection. Administrators should re-enable logging, validate heap check counters (show checkheaps), and investigate any anomalies such as missing logs or frozen counters, as these are strong indicators of compromise.



Validate Device Integrity and Persistence Attempts: Compromise has been linked to bootloader and ROMMON tampering for persistence. After upgrades, check for suspicious artifacts like firmware_update.log and monitor console output for failed “Verifying bootloader/ROMMON” messages. Any persistence evidence should be treated as a high-confidence compromise requiring device rebuild or replacement.



Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0042</u> Resource Development
<u>TA0005</u> Defense Evasion	<u>TA0040</u> Impact	<u>TA0004</u> Privilege Escalation	<u>T1529</u> System Shutdown/Reboot
<u>T1190</u> Exploit Public-Facing Application	<u>T1078</u> Valid Accounts	<u>T1542.001</u> System Firmware	<u>T1542</u> Pre-OS Boot
<u>T1543</u> Create or Modify System Process	<u>T1562</u> Impair Defenses	<u>T1070</u> Indicator Removal	<u>T1542.003</u> Bootkit
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1588</u> Obtain Capabilities
<u>T1059</u> Command and Scripting Interpreter			



Patch Link

https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks



References

<https://unit42.paloaltonetworks.com/zero-day-vulnerabilities-affect-cisco-software/>

<https://www.tenable.com/blog/cve-2025-20333-cve-2025-20362-faq-cisco-as-a-ftd-zero-days-uat4356>

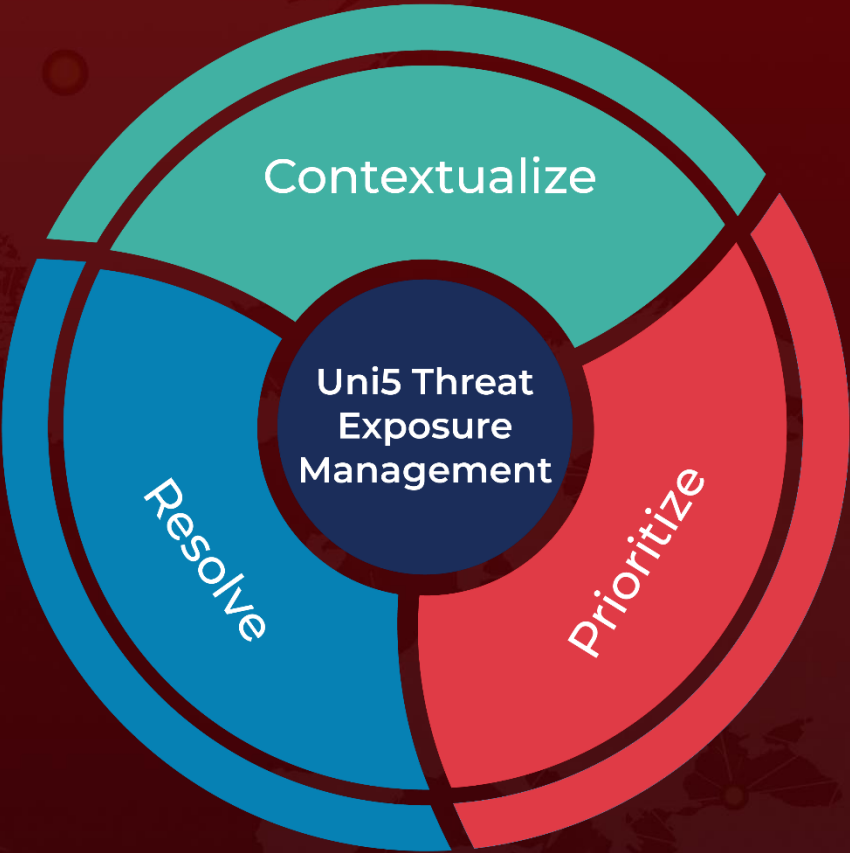
<https://www.hivepro.com/threat-advisory/arcanedoor-a-novel-espionage-campaign-exploits-cisco-zero-days/>



What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

September 29, 2025 • 11:30 PM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com