Hive Pro

Threat Level

Red

CISA: AR26-113A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

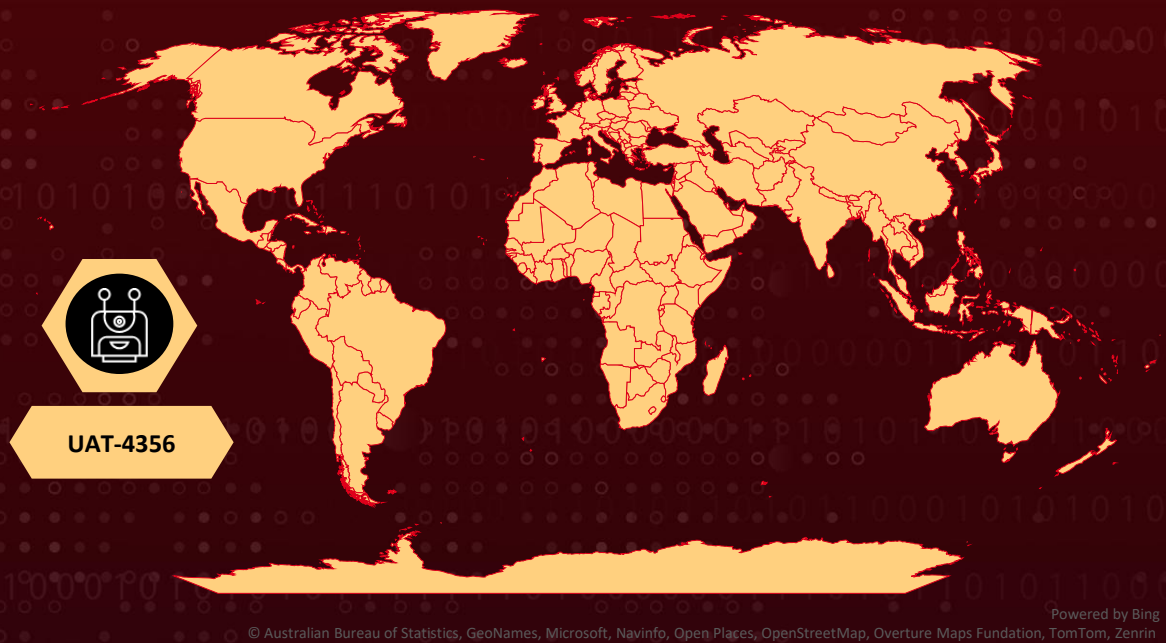
Patched but Not Cured: FIRESTARTER Backdoor Survives Cisco Firewall Upgrades

Date of Publication	Admiralty Code	TA Number
April 27, 2026	A1	TA2026115

Summary

First Seen: September 2025
Attack Commended: March 2026
Targeted Regions: Worldwide
Targeted Platforms: Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower eXtensible Operating System (FXOS)
Targeted Industries: Government, Critical Infrastructure, and Telecommunications (any organization with internet-facing Cisco ASA, FTD, or Firepower VPN web services)
Threat Actor: UAT-4356 (aka Storm-1849)
Malware: FIRESTARTER, LINE VIPER, RayInitiator
Attack: UAT-4356 actors exploited two vulnerabilities (CVE-2025-20333 and CVE-2025-20362) in the VPN web server of Cisco Secure Firewall ASA and FTD software to gain unauthenticated remote access and remote code execution on internet-facing devices. After initial compromise, the actors deployed the LINE VIPER user-mode shellcode loader to establish illegitimate VPN sessions and harvest device configuration, administrative credentials, certificates, and private keys. Subsequently, they implanted FIRESTARTER, a Linux ELF backdoor, which hooks into the LINA process on the firewall and modifies the Cisco Service Platform mount list (CSP_MOUNT_LIST) to maintain persistence. Critically, FIRESTARTER survives firmware updates, security patches, and graceful reboots, allowing the threat actor to retain access to compromised devices long after remediation actions are taken.

Attack Regions



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	Cisco Secure Firewall ASA and FTD Software	✓	✓	✓
CVE-2025-20362	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	Cisco Secure Firewall ASA and FTD Software	✓	✓	✓

Attack Details

#1

A sophisticated state-sponsored threat actor tracked as UAT4356, also known as Storm-1849 and the operator behind the ArcaneDoor campaign, has returned with an evolved attack chain targeting Cisco Secure Firewall ASA, Firepower Threat Defense, and Firepower platforms. The actor specializes in long-term compromise of internet-facing perimeter devices for espionage, exploiting the limited visibility and infrequent patching of network appliances. The 2026 evolution introduces a previously undocumented backdoor named FIRESTARTER, which materially changes the threat picture for any organization that operated exposed Cisco firewall infrastructure prior to September 2025.

#2

The attack chain begins with chained exploitation of CVE-2025-20333 and CVE-2025-20362 against internet-facing WebVPN interfaces, yielding unauthenticated remote code execution as root. The actor then deploys LINE VIPER, a user-mode loader providing command execution, packet capture, credential theft, and bypass of authentication, authorization, and accounting policies. On legacy devices, RayInitiator is additionally deployed as a bootkit. Across all supported platforms, FIRESTARTER is dropped as the primary persistence implant.

#3 FIRESTARTER is a Linux ELF binary that hooks the LINA process. During graceful shutdown, it intercepts the termination signal, copies itself to a secondary location, and rewrites the Cisco Service Platform mount list (CSP_MOUNT_LIST) to ensure re-execution on next boot. After boot, it restores the original mount list, leaving minimal forensic trace. This routine survives reboots, reloads, and firmware upgrades; only a hard power cycle interrupts it, and that is not a recommended remediation due to data corruption risk.

#4 Once installed, FIRESTARTER lies dormant, generating no outbound traffic, no log events, and no behavioral anomalies. It waits for a crafted WebVPN authentication request containing a "magic packet" payload, then parses an embedded XML-based shellcode and executes the operator's payload, typically redeploying LINE VIPER. Critically, this re-entry path requires no re-exploitation of any CVE: a fully patched device compromised before the patch window remains accessible indefinitely. Confirmed dwell time at one breached organization exceeded six months. Patching is now necessary but insufficient; forensic hunting and reimaging are required to evict the actor.

Recommendations

- **Apply Cisco Fixed Software Releases for ASA and FTD:** Upgrade all Cisco Secure Firewall ASA and FTD devices to the fixed software releases listed in Cisco's security advisory for CVE-2025-20333 and CVE-2025-20362. Devices that are not yet patched, or that were updated to a still-vulnerable software version, must be moved to the explicitly listed fixed releases.

- **Reimage Devices to Remove FIRESTARTER:** It's strongly recommended that reimaging and upgrading any device suspected of compromise. Reimaging is the only fully reliable method to remove the FIRESTARTER persistence mechanism on confirmed-compromised devices, and Cisco recommends it for both compromised and non-compromised cases.

- **Hard-Power-Cycle Compromised Devices When Reimage Is Not Immediately Possible:** Physically unplug the affected device from all power sources (including redundant power) for at least one minute. The shutdown, reboot, and reload CLI commands will not clear the in-memory implant — only complete power loss will. This is a temporary mitigation; reimaging must still follow.

- **Hunt for FIRESTARTER on Cisco ASA and Firepower Devices:** Run `show kernel process | include lina_cs` on every Cisco ASA / Firepower / Secure Firewall device. Any output should be treated as a confirmed compromise. Also inspect the disk for /usr/bin/lina_cs and /opt/cisco/platform/logs/var/log/svc_samcore.log, noting that attackers can rename these artifacts.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
Defense Evasion	T1070: Indicator Removal	
	T1222: File and Directory Permissions Modification	
	T1564: Hide Artifacts	
	T1070: Indicator Removal	T1070.004: File Deletion
		T1070.006: Timestomp
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1055: Process Injection	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Persistence	T1543: Create or Modify System Process	
	T1078: Valid Accounts	
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
	T1547: Boot or Logon Autostart Execution	

Tactic	Technique	Sub-technique
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Command and Control	T1219: Remote Access Software	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1070.004: File Deletion
Execution	T1059: Command and Scripting Interpreter	
Collection	T1005: Data from Local System	

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	/usr/bin/lina_cs, /opt/cisco/platform/logs/var/log/svc_samcore.log, /opt/cisco/config/platform/rmdb/CSP_MOUNT_LIST, /opt/cisco/config/platform/rmdb/CSP_MOUNT_LIST.tmp

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

References

https://www.cisa.gov/news-events/news/cisa-warns-firestarter-malware-targeting-cisco-asa-including-firepower-and-secure-firewall-products

https://www.cisa.gov/news-events/analysis-reports/ar26-113a

https://blog.talosintelligence.com/uat-4356-firestarter/

https://hivepro.com/threat-advisory/active-zero-day-exploitation-on-cisco-asa-and-ftd-devices/

https://www.ncsc.govt.nz/alerts/firestarter-malware-affecting-cisco-asa-and-ftd/

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 Demo of **HivePro**.

REPORT GENERATED ON

April 27, 2026 • 04:30 AM

More at www.hivepro.com