Technical Companion

Companion to: Cisco ASA/FTD Firewalls Backdoored by Nation-State Actor — Patching Alone Does Not Remove the Threat

Reference Bulletin Date: April 28, 2026 | For internal use and client technical response

Commands & Syntax Notice: Commands and code in this document are reproduced from cited sources as a reference only. Results may vary based on your environment, OS version, and tooling. Validate in a test environment before running in production.

IOC Notice: Indicators listed here reflect those reported by cited sources at time of publication and are not exhaustive. Threat actor infrastructure evolves — consult current threat intelligence feeds and your EDR/SIEM for the most complete picture. Absence of these indicators does not confirm a clean environment.

1. Patch Verification

Complete all steps below. Steps 1 and 2 address initial access CVEs. Step 3 addresses the FIRESTARTER persistence layer specifically — it is a separate, additional update.

Step 1 — Verify Patch Status for CVE-2025-20333 and CVE-2025-20362

- Confirm running ASA software version from device CLI:
  - `show version | include Software Version`
- Confirm running FTD software version (FMC-managed devices):
  - `Navigate to Devices > Device Management > select device > Device tab > Software Version`
- Minimum fixed versions by branch (Source: Cisco Advisory):
  - `ASA 9.12 → 9.12.4.72 or later`
  - `ASA 9.14 → 9.14.4.28 or later`
  - `ASA 9.16 → 9.16.4.85 or later`
  - `ASA 9.17 → migrate to supported branch`
  - `ASA 9.18 → 9.18.4.67 or later`
  - `ASA 9.19 → migrate to supported branch`
  - `ASA 9.20 → 9.20.4.10 or later`
  - `ASA 9.22 → 9.22.2.14 or later`
  - `ASA 9.23 → 9.23.1.19 or later`
  - `FTD 7.0 → 7.0.8.1 or later`
- Download fixed software from Cisco's Software Download portal:
  - `https://software.cisco.com/download/home`
- Confirm Snort rules are active for CVE-2025-20333 (rule 65340) and CVE-2025-20362 (rule 46897) if running Cisco IDS/IPS (Source: Cisco Advisory).

Step 2 — Apply FIRESTARTER Persistence-Specific Patch (April 2026)

- This patch addresses the FXOS-layer persistence mechanism and is separate from the September 2025 CVE patches. Cisco released it in conjunction with the April 23, 2026 CISA advisory update (Source: Cisco Advisory).
- Obtain the FXOS-layer update for your specific hardware platform via:

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

- Apply update per Cisco's upgrade guidance for your platform. Then perform a hard power cycle — physically unplug the device's power supply. Do not rely on a standard reboot (Source: CISA ED 25-03 V1).

Step 3 — Run Tenable Plugins

- Run Plugin 265943 to detect CVE-2025-20333 exposure on ASA/FTD devices:
  - https://www.tenable.com/plugins/nessus/265943 (Source: Tenable)
- Run Plugin 265966 to detect CVE-2025-20362 exposure on ASA/FTD devices:
  - https://www.tenable.com/plugins/nessus/265966 (Source: Tenable)
- A clean scan result confirms patch coverage for initial access CVEs but does NOT confirm FIRESTARTER has been removed — complete Steps 1-2 above regardless.

2. Compromise Detection / Threat Hunt

Check 1 — CLI Quick Check for FIRESTARTER Process

Run from the ASA/FTD privileged exec prompt. An output line containing lina_cs indicates active FIRESTARTER presence (Source: CISA AR26-113A).

- `show kernel process | include lina_cs`
- No output = lina_cs process not detected. Does not definitively rule out compromise — proceed with core dump analysis.
- Output present = treat as confirmed compromise. Immediately follow Incident Response steps in Section 5.

Check 2 — WebVPN Customization Audit

LINE VIPER can abuse the AnyConnect WebVPN customization mechanism. Audit for unexpected files (Source: CISA ED 25-03).

- Run the following command and review all output for .pdf or .bat files not validated as legitimate:
  - `show import webvpn AnyConnect-customization`
- Examine running-config and startup-config for unauthorized changes — look for new user accounts, modified AnyConnect WebVPN client configuration, unfamiliar IPSec tunnels, or settings that reduce security (e.g., Telnet enabled, weak SNMP).

Check 3 — CISA Core Dump and Hunt Procedure

This is the definitive detection method. Required for all devices meeting CISA's scope criteria (Source: CISA ED 25-03 V1).

- Follow CISA's step-by-step Core Dump and Hunt Instructions (Parts 1–3) at:
  - https://www.cisa.gov/news-events/directives/v1-ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
- Submit core dump via the CISA Malware Next-Gen Analysis portal per the instructions in the directive.
- If CISA returns 'Compromise Detected': immediately disconnect the device from the network (do NOT power off), report to CISA, and initiate incident response. For healthcare clients, begin HIPAA breach analysis immediately.

Check 4 — YARA Rules Against Disk Image or Core Dump

CISA published two YARA rules in Malware Analysis Report AR26-113A that detect FIRESTARTER in disk images and core dumps (Source: CISA AR26-113A).

- Download the YARA rules from AR26-113A at:
  - `https://www.cisa.gov/news-events/analysis-reports/ar26-113a`
- Apply rules against disk images or core dumps using a standard YARA scanner:
  - `yara firestarter_rules.yar <core_dump_file_or_image>`

3. IOC Reference Table

The following indicators are derived from CISA AR26-113A and the Cisco Security Advisory. Verify these against your environment, SIEM, and firewall logs.

Type	Indicator	Description	Source
File Path	`/opt/cisco/platform/logs/var/log/svc_samcore.log`	FIRESTARTER secondary copy — malware writes itself here as part of persistence restoration routine	CISA AR26-113A
File Path	`/usr/bin/lina_cs`	FIRESTARTER primary binary location — restored from secondary copy on reboot	CISA AR26-113A
Config Key	`CSP_MOUNT_LIST`	Cisco Service Platform mount list — FIRESTARTER modifies this to ensure lina_cs executes at boot	CISA AR26-113A / Cisco Advisory
Process Name	`lina_cs`	FIRESTARTER process; detectable via 'show kernel process | include lina_cs'	CISA AR26-113A
Network Trigger	`Crafted WebVPN HTTPS request with hardcoded identifier`	Covert C2 trigger — activates shellcode execution via modified LINA XML handler; no public signature released	CISA AR26-113A
Malware Family	`LINE VIPER (pre-FIRESTARTER)`	User-mode shellcode loader; establishes VPN sessions using dormant accounts; exfiltrates config, credentials, certs, and private keys	CISA AR26-113A

Note: No public network-layer PCAP signatures or IP/domain IOCs have been published for FIRESTARTER at this time. Monitor for anomalous WebVPN session activity and unexpected VPN tunnel creation from dormant accounts.

4. Credential and Certificate Rotation Scope

If any in-scope device cannot be confirmed clean, treat all credentials stored on or transiting that device as compromised. LINE VIPER is purpose-built to exfiltrate this data (Source: CISA AR26-113A).

Credentials to Rotate

- All local ASA/FTD admin and read-only accounts.
- TACACS+ and RADIUS service account credentials used for device authentication.
- SNMP community strings and v3 credentials.
- Any break-glass or emergency access accounts with device access.

Certificates and Keys to Replace

- SSL/TLS certificates bound to WebVPN/AnyConnect — replace with newly issued certificates from your PKI or CA.
- IPSec pre-shared keys and IKEv1/v2 secrets for site-to-site VPN tunnels terminated at affected devices.
- VPN client certificates provisioned from the affected device's CA.
- Private keys stored in device trustpoints — verify via:
  - `show crypto key mypubkey rsa`

VPN Account Audit

- Identify dormant VPN user accounts — LINE VIPER specifically leveraged accounts that existed but were not actively monitored.
- Run a report of all VPN accounts with last-login older than 90 days and disable any that cannot be validated as needed.
- Review authentication logs for any VPN sessions that occurred from unexpected source IPs or during off-hours in the September–April timeframe.

5. Incident Response Triggers and Escalation

Confirm Compromise — Immediate Actions

- If the CLI check (lina_cs process detected) OR core dump returns 'Compromise Detected': disconnect the device from the network immediately — do NOT power it off, as powering off may complicate forensic analysis (Source: CISA ED 25-03 V1).
- Preserve a core dump before any further remediation steps. Submit to CISA via the Malware Next-Gen portal.
- Notify CISA via the incident reporting portal and engage Cisco TAC for incident-specific support.

Healthcare-Specific Escalation

- Initiate HIPAA breach determination analysis immediately — a confirmed perimeter device compromise may constitute a breach if patient data was accessible through network segments protected by the device.
- Begin the HHS OCR 60-day notification clock from the date compromise is confirmed, not the date of initial exploitation (unless the exploitation date can be established with certainty).
- Preserve all logs and forensic artifacts in accordance with legal hold obligations — do not perform remediation steps that destroy evidence without first completing preservation.

Hardening: Reduce Future Attack Surface

- Disable WebVPN and AnyConnect on devices where remote access VPN is not an operational requirement — CVE-2025-20362 and CVE-2025-20333 require WebVPN to be enabled and accessible.
- Restrict management access to ASA/FTD devices to a dedicated out-of-band management network — prevent direct internet access to management interfaces.
- Implement TACACS+ over TLS 1.3 for all device administration to encrypt authentication traffic and reduce credential interception risk (Source: CISA ED 25-03 V1 / Cisco).
- Enable Secure Boot where hardware supports it — Cisco confirmed FIRESTARTER's persistence mechanism does not affect Secure Boot-capable devices (Source: Cisco Advisory).