INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 18:50 UTC

ArcaneDoor's Firestarter Implant Survives Patching: Cisco Firewall Compromise Demands Physical Remediation

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0212
Type	Threat Campaign
CVE ID	CVE-2025-20333, CVE-2025-20362
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.2221 (96th percentile)
Affected Products	Cisco Secure Firewall ASA and FTD on Firepower 1000, 2100, 4100, 9300 Series; Cisco Secure Firewall 1200, 3100, 4200 Series
Published	2026-04-23T15:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

China-nexus threat actor ArcaneDoor (UAT-4356) has deployed a firmware-level implant called Firestarter on Cisco Secure Firewall ASA and FTD devices that survives software patches and reboots. CISA confirmed active exploitation on a U.S. federal civilian agency device via Emergency Directive on April 23, 2026, rendering September 2025 patches insufficient for full remediation, as the implant persists at firmware layer (FXOS) beneath the patched software stack. Organizations running affected Cisco Firepower and Secure Firewall hardware must physically power-cycle or reimage devices to achieve full remediation; patch-and-reboot procedures leave compromised devices persistently backdoored.

Technical Analysis

Firestarter is a firmware-resident implant embedded in FXOS, the underlying OS beneath Cisco ASA and FTD software stacks. Because FXOS persists across software-layer operations, the implant survives OS upgrades, hotfixes, and standard reboots. Affected hardware includes Cisco Secure Firewall ASA and FTD on Firepower 1000, 2100, 4100, and 9300 Series, plus Cisco Secure Firewall 1200, 3100, and 4200 Series. The campaign exploits CVE-2025-20333 and CVE-2025-20362 (CVSS 9.5), with EPSS at 0.2221 (95th percentile), indicating high observed exploitation probability. Relevant CWEs include CWE-78 (OS command injection), CWE-284

(improper access control), CWE-20 (improper input validation), and CWE-693 (protection mechanism failure). MITRE ATT&CK techniques include T1542.003 (Bootkit), T1601 (Modify System Image), T1600 (Weaken Encryption), T1190 (Exploit Public-Facing Application), T1070 (Indicator Removal), T1556 (Modify Authentication Process), T1557 (Man-in-the-Middle traffic interception at firewall layer), and others mapped in the metadata. Cisco's security advisory confirms that full remediation requires either complete device reimaging or physical power disconnection; software patching alone is insufficient.

Action Checklist

1. Step 1: Containment. Immediately isolate all affected Cisco Secure Firewall ASA and FTD devices on Firepower 1000, 2100, 4100, 9300, and Secure Firewall 1200, 3100, 4200 Series from internet-facing network segments. Do not trust patch-and-reboot status as confirmation of clean state. Treat any device that was unpatched prior to September 2025 and has not been reimaged as potentially compromised.
2. Step 2: Detection. Audit FXOS integrity using Cisco's secure boot and software integrity verification features per the Cisco Security Advisory (cisco-sa-asaftd-persist-CISAED25-03). Review syslog output for unexpected process creation, authentication anomalies, and configuration changes consistent with T1070 (log clearing) and T1556 (auth modification). Correlate management-plane access logs against known-good baselines. Check for unexpected outbound connections from firewall management interfaces.
3. Step 3: Eradication. Per Cisco's advisory and CISA Emergency Directive (April 23, 2026, CISAED25-03), full remediation requires one of two actions: (a) complete device reimaging using verified clean firmware obtained directly from Cisco's official distribution channels, or (b) physical power disconnection (not software reboot). Software patches applied September 2025 do not eradicate Firestarter. Verify firmware integrity post-reimage using Cisco's Trust Anchor module verification process.
4. Step 4: Recovery. After reimaging, restore device configurations from a known-clean backup predating the suspected compromise window. Rotate all credentials associated with affected devices, including VPN keys, management accounts, and any service accounts with firewall API access. Monitor post-reimage for re-exploitation attempts targeting CVE-2025-20333 and CVE-2025-20362, and validate that the latest Cisco ASA/FTD software versions are applied.
5. Step 5: Post-Incident. Conduct a gap assessment against NIST SP 800-53 controls SI-7 (Software, Firmware, and Information Integrity) and CM-6 (Configuration Settings). Evaluate whether firmware integrity monitoring is integrated into your continuous monitoring program. Review network segmentation controls limiting lateral movement from perimeter devices. Assess whether FXOS-layer attestation is part of your hardware lifecycle policy. Report to CISA if you identify Firestarter on any federal or critical infrastructure device, per Emergency Directive requirements.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, legal counsel, and CISA if any Firepower or Secure Firewall device shows FXOS integrity check failures, confirms presence of Line Dancer or Line Runner artifacts, or is identified as a federal civilian agency asset subject to the April 23, 2026 CISA Emergency Directive — active nation-state exploitation with firmware persistence and a CVSS 9.5 rating on internet-facing perimeter devices constitutes a Severity 1 incident with mandatory regulatory reporting timelines.

Recovery Notes	Post-reimage validation must include FXOS Trust Anchor module attestation and side-by-side hash verification against Cisco's published golden firmware hashes before any reimaged device is returned to production — do not rely on software reboot alone given Firestarter's documented persistence mechanism. Monitor reimaged devices for at least 30 days using enhanced syslog verbosity forwarded to an out-of-band syslog server, specifically watching for re-appearance of the MITRE T1556 and T1070 TTPs ArcaneDoor used in the original campaign. Given ArcaneDoor's (UAT-4356) known interest in VPN and perimeter device credentials, treat all VPN session keys, tunnel group pre-shared keys, and management API tokens as fully compromised and verify downstream systems accessed via VPN tunnels through these devices for signs of lateral movement.
Forensic Artifacts	FXOS 'show platform software integrity' output with SHA-256/SHA-512 hash values for boot components — the primary indicator of Firestarter persistence below the ASA/FTD OS layer, as the implant modifies FXOS boot image components that survive software-only patches and warm reboots | ASA/FTD syslog message IDs 111008 and 111009 (configuration change events) and 605005 (AAA/management authentication events) from the period preceding September 2025 patching through isolation — ArcaneDoor's Line Dancer implant modified authentication configurations consistent with MITRE T1556 and may have cleared logs consistent with T1070, making timestamp gaps themselves a forensic artifact | Full ASA/FTD running-config and startup-config snapshots diffed against the last known-clean backup — specifically hunting for unauthorized local user accounts (T1136.001), modified aaa-server group configurations, added crypto map or tunnel-group entries indicating unauthorized VPN establishment, and 'service internal' commands exposing hidden management interfaces used by Line Runner | NetFlow records or SPAN/mirror captures from the management interface (Management0/0 or Firepower chassis MGMT port) covering the full suspected dwell period — Firestarter beacons outbound for C2 and ArcaneDoor is documented to exfiltrate configuration data and credentials, making unexplained outbound sessions from the management plane the highest-fidelity network-layer indicator | Firepower chassis FXOS audit logs ('show audit-logs' from chassis manager) and 'show processes' snapshots — anomalous FXOS-layer processes or audit log entries showing configuration commits from unexpected source IPs or at unexpected times indicate active implant interaction, as Firestarter operates at the FXOS/OS boundary and may appear as modified or injected FXOS service processes

Per-Action IR Details

Step 1: Containment — Immediately isolate all affected Cisco Secure Firewall ASA and FTD devices on Firepower 1000, 2100, 4100, 9300, and Secure Firewall 1200, 3100, 4200 Series from internet-facing network segments. Do not trust patch-and-reboot status as confirmation of clean state. Treat any device that was unpatched prior to September 2025 and has not been reimaged as potentially compromised.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 — Establish and Maintain a Secure Network Architecture

Compensating: For teams without NAC or automated isolation: immediately apply ACLs on upstream upstream switches/routers to null-route management and outside interface IPs for affected Firepower/Secure Firewall devices. On Cisco IOS upstream devices, execute: 'ip route [firewall-outside-IP] 255.255.255.255 Null0' and 'ip route [firewall-mgmt-IP] 255.255.255.255 Null0'. Simultaneously disable ASDM and SSH access via out-of-band console: 'no http server enable' and 'no ssh [management-subnet] [mask] management'. Document the time of isolation with console-captured timestamps before any further action — this timestamp anchors your compromise window for CISA reporting under the Emergency Directive.

Evidence: Before isolating, capture full NetFlow or SPAN traffic from the firewall's management interface (typically Management0/0 or dedicated MGMT port on Firepower 4100/9300 chassis) for the 72 hours preceding isolation. Specifically look for unexpected outbound TCP/UDP sessions from the management interface to non-Cisco, non-organizational IPs — Firestarter is documented to beacon outbound for C2. Use Wireshark or tcpdump on the upstream switch mirror port: 'tcpdump -i [span-interface] -w firestarter_mgmt_capture.pcap host [firewall-mgmt-IP]'. Export the FXOS platform event log and ASA/FTD system log before isolation disrupts syslog forwarding.

Step 2: Detection — Audit FXOS integrity using Cisco's secure boot and software integrity verification features per the Cisco Security Advisory (cisco-sa-asaftd-persist-CISAED25-03). Review syslog output for unexpected process creation, authentication anomalies, and configuration changes consistent with T1070 (log clearing) and T1556 (auth modification). Correlate management-plane access logs against known-good baselines. Check for unexpected outbound connections from firewall management interfaces.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, perform manual FXOS integrity checks via console: SSH to Firepower chassis manager (FCM) and run 'show platform software integrity' and 'show version' — compare SHA-256 hashes against Cisco's published golden hashes in advisory cisco-sa-asaftd-persist-CISAED25-03. For ASA: run 'show version' and 'verify /sha-512 disk0:[running-image.bin]' and compare output to Cisco's published hash. For FTD on Firepower: use 'system support diagnostic-cli' then 'show disk file list' to enumerate unexpected files in /ngfw/var/sf/ or /mnt/disk0. Export ASA syslogs via 'show logging' filtered for syslog message IDs 106001, 106006, 111008, 111009, 302013–302016 (connection events) and 605005 (AAA authentication failures) to a text file for manual grep analysis.

Evidence: Capture the following before any remediation: (1) FXOS 'show platform software integrity' output with console timestamp — this is the primary artifact confirming whether Firestarter modified boot components below the OS layer. (2) ASA/FTD running configuration snapshot via 'show running-config' — Firestarter and associated ArcaneDoor tooling (Line Dancer, Line Runner) are known to inject backdoor accounts and modify AAA configurations consistent with MITRE T1556.001 (Modify Authentication Process: Domain Controller Authentication). (3) Full syslog buffer: 'show logging buffered' — look for gaps in log timestamps indicating T1070.002 (Indicator Removal: Clear Linux or Mac System Logs) activity. (4) FXOS audit log: 'show audit-logs' from the Firepower chassis manager. (5) Netstat equivalent on FTD: 'show conn all' and 'show local-host all' to enumerate active connections at time of analysis.

Step 3: Eradication — Per Cisco's advisory and CISA Emergency Directive (April 23, 2026), full remediation requires one of two actions: (a) complete device reimaging using verified clean firmware obtained directly from Cisco's official distribution channels, or (b) physical power disconnection (not software reboot). Software patches applied September 2025 do not eradicate Firestarter. Verify firmware integrity post-reimage using Cisco's Trust Anchor module verification process.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without an automated software deployment pipeline: download ASA or FTD firmware image directly from software.cisco.com using a verified, out-of-band workstation (not a host that traverses the compromised firewall). Validate the downloaded image SHA-512 hash before transfer: 'certutil -hashfile [image.bin] SHA512' (Windows) or 'sha512sum [image.bin]' (Linux) — compare against Cisco's published hash in the advisory. Transfer via USB or trusted out-of-band management network only. For Firepower 4100/9300 chassis: connect via console to FXOS and execute a full chassis reimage using 'connect local-mgmt' then follow Cisco's FXOS reimaging procedure, which initializes the Trust Anchor module (TAm) from ROM — this is the only software path that eliminates Firestarter. Physical power disconnect (not 'reload') before reimaging clears volatile implant state if TAm initialization

has been subverted.

Evidence: Before initiating reimaging, preserve the following as forensic evidence: (1) Full flash/disk image of the compromised FXOS partition if forensically feasible — use Cisco TAC guidance to extract disk0 contents via 'copy disk0: tftp:' to an isolated forensic TFTP server. (2) Memory forensics if operationally feasible: Firestarter operates in-memory at the FXOS/OS boundary; capture 'show tech-support' output and 'show processes' with CPU/memory details — these may reveal anomalous FXOS processes injected by the implant. (3) Photograph or log the physical chassis serial numbers and hardware revision markings before and after remediation for chain-of-custody documentation required by the CISA Emergency Directive. (4) Export all configuration backups ('copy running-config tftp:') to confirm what credentials and policy objects an attacker may have exfiltrated or modified.

Step 4: Recovery — After reimaging, restore device configurations from a known-clean backup predating the suspected compromise window. Rotate all credentials associated with affected devices, including VPN keys, management accounts, and any service accounts with firewall API access. Monitor post-reimage for re-exploitation attempts targeting CVE-2025-20333 and CVE-2025-20362, and validate that the latest Cisco ASA/FTD software versions are applied.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation without a PAM solution: generate a new RSA-4096 or ECDSA-256 keypair for SSH management access and replace all ASDM/SSH keys via console before re-enabling remote access: 'crypto key generate rsa modulus 4096 label mgmt-key-post-reimage'. Enumerate all service accounts with firewall REST API access by reviewing the FTD FMC API client list or ASA aaa-server configurations in the pre-compromise config backup — revoke and regenerate each token manually. For VPN certificate rotation: revoke existing ASA identity certificates via your CA, issue new certificates, and re-enroll via SCEP or manual PKCS#12 import. Post-reimage, enable enhanced syslog verbosity ('logging trap debugging' on a test basis) and forward to a syslog server (rsyslog or syslog-ng on a dedicated Linux VM) to establish a new known-good baseline for management-plane activity.

Evidence: Identify the clean configuration backup by correlating backup timestamps against the earliest possible compromise date — ArcaneDoor activity was first observed in late 2023 per Cisco Talos reporting, meaning backups from before November 2023 are the only high-confidence clean baselines. Diff the pre-compromise backup against the last running configuration using 'diff' or a text comparison tool to identify all changes ArcaneDoor tooling may have introduced, including: new local user accounts (T1136.001), modified aaa-server configurations (T1556), added or modified crypto map entries that could indicate unauthorized VPN tunnel establishment, and any 'service internal' commands that expose hidden debug interfaces used by Line Dancer/Line Runner implant infrastructure.

Step 5: Post-Incident — Conduct a gap assessment against NIST SP 800-53 controls SI-7 (Software, Firmware, and Information Integrity) and CM-6 (Configuration Settings). Evaluate whether firmware integrity monitoring is integrated into your continuous monitoring program. Review network segmentation controls limiting lateral movement from perimeter devices. Assess whether FXOS-layer attestation is part of your hardware lifecycle policy. Report to CISA if you identify Firestarter on any federal or critical infrastructure device, per Emergency Directive requirements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without a commercial firmware integrity monitoring platform: schedule quarterly FXOS integrity verification as a documented manual procedure — create a cron job or scheduled task that pulls 'show platform software integrity' output via an authenticated SSH session to each Firepower chassis and compares hashes against a

locally-maintained golden hash registry (a simple CSV mapping device serial to expected FXOS hash). Use Cisco's PSIRT OpenVuln API (free, requires CCO login) to automate ingestion of future ASA/FTD advisories into your vulnerability tracking workflow. Create a Sigma rule targeting your syslog collection for Cisco ASA message IDs 111008/111009 (config changes by non-admin accounts) and 605005 (management auth failures) to detect re-exploitation attempts against CVE-2025-20333 and CVE-2025-20362 post-recovery.

Evidence: Compile the complete incident timeline for the lessons-learned report, anchoring key timestamps to: (1) the September 2025 patch date (previously considered remediated), (2) the April 23, 2026 CISA Emergency Directive date (confirmed exploitation), and (3) your organization's own isolation and reimaging timestamps — this delta represents your maximum attacker dwell time and must be disclosed to CISA if the device is on a federal civilian agency network. Retain all captured syslog buffers, FXOS integrity check outputs, network captures, and configuration diffs for a minimum of 3 years per NIST AU-11 (Audit Record Retention) and CISA ED data retention requirements. Document which credential classes were exposed to the compromised devices to scope any downstream breach notification obligations.

Detection Guidance

Detection must target the FXOS layer, not just ASA/FTD software logs. Use Cisco's software integrity verification commands (show software authenticity, verify /md5) to compare running firmware hashes against Cisco-published golden values. Review FXOS system logs for unexpected module loads, process spawning outside normal boot sequence (T1543), and unauthorized service installations (T1505). Monitor management-plane authentication logs for anomalous access patterns consistent with T1078 (valid account abuse) and T1133 (external remote services). Look for evidence of log clearing (T1070) that may mask implant activity. Network-side: capture and baseline management interface egress traffic; Firestarter-class implants commonly establish covert C2 channels. Behavioral indicators include unexpected FXOS process execution, configuration modifications with no corresponding change ticket, and authentication events from unfamiliar source IPs on management interfaces.

Framework Mappings

MITRE-ATTACK

- **T1542.003** — Bootkit
- **T1557** — Adversary-in-the-Middle
- **T1542** — Pre-OS Boot
- **T1078** — Valid Accounts
- **T1070** — Indicator Removal
- **T1547** — Boot or Logon Autostart Execution
- **T1556** — Modify Authentication Process
- **T1601** — Modify System Image
- **T1600** — Weaken Encryption
- **T1059** — Command and Scripting Interpreter
- **T1543** — Create or Modify System Process
- **T1505** — Server Software Component
- **T1036** — Masquerading

- **T1133** — External Remote Services
- **T1542.001** — System Firmware
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1542.003	Bootkit	Persistence
T1557	Adversary-in-the-Middle	Credential-Access
T1542	Pre-OS Boot	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1070	Indicator Removal	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1556	Modify Authentication Process	Credential-Access
T1601	Modify System Image	Defense-Evasion
T1600	Weaken Encryption	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1543	Create or Modify System Process	Persistence
T1505	Server Software Component	Persistence
T1036	Masquerading	Defense-Evasion
T1133	External Remote Services	Persistence
T1542.001	System Firmware	Persistence
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://cyberscoop.com/cisco-firestarter-malware-cisa-warning/	T3
	https://www.csoonline.com/article/4063518/patch-now-attacker-finds-...	T3

Source	URL	Tier
	https://www.securityweek.com/cisco-firewall-zero-days-exploited-in-...	T3
Cisco Secure Firewall Adaptive Security Appliance Software and ...	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-20333, CVE-2025-20362	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-04-23 18:50 UTC by TJS Security Command Center