CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

V1: ED 25-03: IDENTIFY AND MITIGATE POTENTIAL COMPROMISE OF CISCO DEVICES

SLTT SNAP Call

Date: 4/23/2026

Time: 3:00 PM EST

TLP:GREEN

CISA SLTT SNAP Call

WARNING: This document is UNCLASSIFIED//For Official Use Only (FOUO).

It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS office.

THIS DOCUMENT IS:

TLP:GREEN

TLP:GREEN

Limited disclosure, restricted to the community.

For more information on Traffic Light Protocol Traffic Light Protocol Link

Welcome Logistics & Participation

Meeting Date: 4/23/2026
Meeting Time: 3:00 PM EST

Microsoft Teams: Click here to join meeting

Dial-In (Audio Only):

- **Call-in (audio only):** Meeting ID: 222 471 202 011 280
  - Passcode: yf77qh2W
  - 1 323-741-4166,,415495851#
- **Phone Conference ID:** 415 495 851#

Agenda

Welcome	James Murphy, Cybersecurity Division Cybersecurity and Infrastructure Security Agency
Threat Overview	Jordan Petrich, Cybersecurity Division Cybersecurity and Infrastructure Security Agency
V1 ED 25-03 Background & Recommended Actions	Sarah Alim, Cybersecurity Division Cybersecurity and Infrastructure Security Agency
Core Dump and Hunt Walk-through	Jordan Petrich, Cybersecurity Division Cybersecurity and Infrastructure Security Agency
Agency Q&A	Kwadwo Burgee, Cybersecurity Division Cybersecurity and Infrastructure Security Agency
Closing Remarks	Christopher Marques, Cybersecurity Division Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Welcome

James Murphy
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Threat Overview

Jordan Petrich
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Threat Overview

- CISA is aware of an ongoing exploitation campaign by an advanced threat actor targeting public-facing Cisco Firepower and Secure Firewall devices running Adaptive Security Appliance (ASA) or Firepower Threat Defense (FTD) software.
- Threat actors are using FIRESTARTER—a backdoor that allows remote access and control—to maintain post-patching persistence, enabling threat actors to re-access compromised devices without re-exploiting vulnerabilities.

Threat Overview (cont.)

CISA's analysis identified the following:

- **Initial Access:** CISA assesses, but has not confirmed, that APT actors obtained initial access by exploiting CVE-2025-20333 and/or CVE-2025-20362 [T1190]. CISA has not confirmed the exact date of initial exploitation but assesses the compromise occurred as early as Sept. 8, 2025, and before the agency implemented patches in accordance with ED 25-03.
- **Privilege Escalation and Defense Evasion:** CISA identified that APT actors first deployed LINE VIPER to establish illegitimate virtual private network (VPN) sessions [T1133] that bypassed all VPN authentication policies. This activity was associated with user accounts that existed but were no longer active within the agency [T1078]. While observed in this incident, threat actors may use other (including fabricated) accounts.
  - LINE VIPER enabled APT actors access to all configuration elements of the victim Firepower device, including administrative credentials, certificates, and private keys [T1082].
- **Persistence:** APT actors deployed FIRESTARTER on the Firepower device before Sept. 25, 2025 (exact date is unknown). Because it was present before patching, FIRESTARTER persisted through remediation and established command and control (C2) channels on the victim Firepower device [T1219].
  - APT actors leveraged FIRESTARTER to regain access without re-exploiting the original vulnerabilities and deployed LINE VIPER on March 12, 2026.

CVEs and KEV Additions

- CISA analysis continues to assess that the following CVEs pose an unacceptable risk to government information systems:
  - CVE-2025-20333 – allows for remote code execution
  - CVE-2025-20362 – allows for privilege escalation

- Although Cisco's patches addressed these CVEs, devices compromised prior to patching may remain vulnerable because FIRESTARTER is not removed by firmware updates.
  - Cisco will be releasing a hotfix for the persistence ("FIRESTARTER") issue on 4/23, which **all entities should apply on Firepower and Secure Firewall devices.**

V1 Background & Recommended Actions

Sarah Alim
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Background

- This V1 supersedes the recommended actions in Emergency Directive (ED) 25-03: Identify and Mitigate Potential Compromise of Cisco Devices and applies to any entity running affected products. **V1 expands on the original ED 25-03 requirements with actions three, four, five, and six.**
- V1 is in response to updated cyber threat intelligence concerning of threat actors retaining persistence and continued unauthorized access to Cisco Firepower and Secure Firewall products with ASA or FTD software.
- CISA analysis determines that applying the Cisco-provided security updates recommended by the original issuance of ED 25-03 does not necessarily remove an existing threat actor from the compromised device.
- Organizations who have completed the security updates are still susceptible to persistence and therefore must complete the updated recommended actions V1.

*Note: These actions are designed and required for FCEB agencies, but CISA highly recommends SLTT partners follow them as well.

Technical Details

- **Original ED 25-03 Scope:**
  - ASA hardware (5512-X, 5515-X, 5525-X, 5545-X, 5555-X, and 5585-X)
  - ASA-Service Modules (ASA-SM)
  - ASA Virtual (ASAv)
- **V1 ED 25-03 Updated Scope:**
  - Cisco Firepower (1000, 2100, 4100, 9300)
  - Cisco Secure Firewall (200, 1200, 3100, 4200 and 6100)

Recommended Actions

V1 recommendations expand on ED 25-03 Actions. Recommendations 1 and 2 remain unchanged. Agencies who have completed these recommendations may move on to Recommended Actions 3 and 4.

For all public-facing Cisco ASA devices:

1. Immediately identify all Cisco ASA platforms (ASA hardware, ASA-Service Module [ASA-SM], ASA Virtual [ASAv]).
2. For instances identified in recommended action #1, follow CISA's step-by-step Core Dump and Hunt Instructions Parts 1-3 and submit core dump(s) via the Malware Next Gen portal.
    a. If the result is "Compromise Detected," organizations must immediately disconnect the device from their network (but do not power off), report the incident to CISA, and work with CISA on incident response and eviction actions.
    b. If the result is "No Compromise Detected,":
        i. For ASA hardware models with an end-of-support date on or before September 30, 2025:
            1. Permanently disconnect these devices on or before September 30, 2025, as these legacy platforms/releases cannot meet current vendor support and update requirements.
            2. Entities that cannot meet this recommendation should apply the latest Cisco-provided updates for software.
        ii. For ASA hardware models with an end-of-support date of August 31, 2026: Download and apply the latest Cisco-provided updates for software and apply all subsequent updates via Cisco's download portal.
        iii. [New Recommendation] For any newly identified ASA hardware models, follow the recommendations outlined in BOD 26-02: Mitigating Risk From End-of-Support Edge Devices.
    c. For all ASAv instances identified in recommended action 1, download and apply the latest Cisco-provided updates for software and apply all subsequent updates via Cisco's download portal.

Recommended Actions (cont.)

For all public-facing Cisco Firepower and Secure Firewall Devices:

1. [New Recommendation] Immediately identify all Firepower 1000, 2100, 4100, 9300 series and Secure Firewall 200, 1200, 3100, 4200, and 6100 series devices.
2. [New Recommendation] For devices identified in recommended action #3, follow CISA's step-by-step Core Dump and Hunt Instructions and submit core dump(s) via the Malware Next Gen portal.
    a. If the result is "Compromise Detected," organizations should: keep the device powered on, immediately disconnect the device from their network, and report the incident to CISA, and work with CISA on incident response, forensics, and eviction actions.

Recommended Actions (cont.)

b. If the result is “No Compromise Detected,” agencies should:
   i. Download and apply the latest Cisco-provided updates for software. This includes:
      1. The software updates to address CVE-2025-20333 and CVE-2025-20362, if not already patched; and,
      2. The recently released patch created for this specific persistence issue (links provided in CISA’s step-by-step Core Dump and Hunt Instructions).
   ii. Perform a hard reset of the device(s) by physically unplugging the device’s power supply, as a reboot is not sufficient to expunge the malware.
      1. Follow CISA’s step-by-step Core Dump and Hunt Instructions, which includes further guidance if a hard reset of the device cannot occur immediately after patch implementation.
   iii. Apply all subsequent updates via Cisco’s download portal.

CISA Actions

1. CISA will continue efforts to identify instances and potential compromises associated with this threat activity, provide partner notifications, and will issue additional guidance and direction, as appropriate.
2. CISA will accept core dumps from SLTT organizations and can provide clarifications to any questions.

Additional Information

- Visit https://www.cisa.gov/news-events/directives or contact the following for:
  - General information and assistance – CyberliaisonsItt@cisa.dhs.gov
  - Reporting indications of compromise – contact@cisa.dhs.gov
- For more information on the threat actor activity, malware functionality, detection methods, and mitigations please see CISA's FIRESTARTER Backdoor Malware Analysis Report https://www.cisa.gov/news-events/analysis-reports/ar26-113a
- For further instructions on how to perform a "core dump" please visit https://cisa.gov/news-events/directives/supplemental-direction-ed-25-03-core-dump-and-hunt-instructions
- For eviction guidance please visit https://www/cisa.gov/eviction-strategies-tool/create-from-template

Core Dump and Hunt Walk-through

Jordan Petrich
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Supplemental Guidance

- The supplemental Core Dump and Hunt Guidance is being provided to help entities check the status of their Cisco devices. It is prudent that all network defenders follow the listed guidance exactly and contact CISA, if signs of compromise are observed.
- Most changes made to the guidance are for Firepower and Secure Firewall devices. Key parts include:
  - Specific commands to run before obtaining a core dump.
  - Core dump instructions
  - Patching guidance (including implementation of Cisco's latest hotfixes)
  - Hard restart guidance
- Additional hunt guidance was also added based on new findings.

Q&A

Kwadwo Burgee
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Closing Remarks

Chris Marques
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency

TLP:GREEN

Visit https://www.cisa.gov/news-events/directives or contact the following for:

- General information, assistance, and reporting – CyberLiaisonSLTT@cisa.dhs.gov
- Reporting indications of potential compromise – Contact@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY