04/23/2026 Meeting Minutes – CISA SLTT SNAP SOC Call

These meeting minutes are intended for use by the attendees of the SNAP version of the SLTT Security Operations Center (SOC) Call as a reference document. See slides included in the Meeting Minutes email.

TLP:GREEN

Main Discussion

- **Emergency Directive (ED) 25-03: Identify and Mitigate Potential Compromise of Cisco Devices**
  - See slides 6-20
  - **Question:** I see instructions for Collecting Core Dumps for Firepower 1000/2100/4100/9300s. I do not see instructions for the Secure Firewall 1200 Threat Defense Series devices. Is there a recommendation what instructions to use?
    - **CISA:** Follow the instructions for 1000/2100 Secure Firewalls (all models); the core dump process is the same.
  - **Question:** If the initial IOC check and the new IOC check were both negative, does that change the recommended timeline to apply the latest hotfix?
    - **CISA:** We recommend applying the hotfix as quickly as possible. If you run the necessary commands and core dumps but require additional time to apply the hotfix and other mitigations, we advise rerunning the commands and submitting updated core dumps. Although running these checks should confirm the device is clean and prevent reinfection, but given the sophistication of this threat, we are going to be overly cautious. Therefore, apply the patch and complete mitigation steps immediately after confirming your device is clean.
  - **Question:** If an FTD device is in HA mode. Do I unplug both firewalls at same time?
    - **CISA:** You may to unplug them at the same time or sequentially to avoid down time.
  - **Question:** If we performed the core dumps back in September, found no detections in our checks, and updated to unaffected versions; do we need to repeat the core dumps again to check for Firestarter in this instance?
    - **CISA:** In September, there was no Firestarter detection mechanism, so compromise wouldn't have occurred then. Regardless of when you patched, if you were ever vulnerable to those CVEs, repeat the core dump, check for Firestarter, and follow the entire process.
  - **Question:** Are there any concerns about firewalls being in a high availability pair or can we address each firewall individually?
    - **CISA:** You can address each firewall individually; take them down one at a time.
  - **Question:** Will there be any patch forthcoming?
    - **CISA:** Cisco has released patches for both FTD firmware and ASA firmware, along with FX OS version upgrades to mitigate this vulnerability. We also recommend continuing to follow the directive and performing a hard reboot as an additional precaution. Please note that version 10.0 of FTD is scheduled for release on April 30th; it is the only version currently without a hotfix available. Also, if you are using FX OS, you will need to upgrade first and then upgrade the ASA FTD firmware which specifically applies for 2100 and 9300 Firepower devices.
  - **Question:** Is the ASA 5508-X affected by Firestarter? It is only used for VPN services.

        - **CISA:** No
    - **Question:** Any info on the exact threat vector is taking to compromise the device?
        - **CISA:** Our analysis indicates the threat actor used two CVEs released in September to access devices. This remains true for devices where we found Firestarter even after patching the CVEs.
    - **Question:** Should we be applying the hotfix even if the current versions of the FTDs are not listed as vulnerable?
        - **CISA:** Yes, you should be applying the hotfix if its available.
    - **Question:** Are critical infrastructure industries being targeted?
        - **CISA:** While we have not observed explicit targeting or found evidence of compromise within critical infrastructure sectors, threat actors consistently attempt to breach infrastructure companies and organizations. Therefore, we strongly recommend applying CISA guidance and relevant hot fixes in this situation. Critical infrastructure is always at risk, so it important to always be prepared.
    - **Question:** In relation to the hard reset, are you asking us to crash the FW by unplugging the power during powered operation. Or shutting down the FW and then removing the power.
        - **CISA:** This procedure should be followed during normal operations. When disconnecting the device, there may be two power sources or redundant power supplies; ensure both are unplugged, wait one minute, and then reconnect them. Only perform this task during normal operation, not after a shutdown.
    - **Question:** How long do we need to keep them unplugged?
        - **CISA:** One minute
    - **Question:** If we are not using and have not used any Cisco Endpoint VPN features (disabled) which as I understand are not impacted by the two CVEs, are we still potentially impacted?
        - **CISA:** We have not observed successful compromises in cases where a web VPN was not enabled on these types of devices. However, it remains unclear whether the same vulnerabilities could be accessed through other services that may be deployed. We continue to recommend following our guidance as a precaution. Regardless of whether it is determined that these devices are not vulnerable to the FTD, we strongly advise applying patches for those CVEs.

Closing Remarks TLP:GREEN

- **Upcoming Technical Exchanges**
    - 05/13/26 – SLTT SOC Call
- **Contact Information**
    - If you have Agenda topics, please send an email request for approval to cyberliaisonsltt@cisa.dhs.gov with your contact information.
    - Contact information needed for additions: Name, Agency, and email address.
    - To report an incident to CISA: Report to CISA | CISA (https://www.cisa.gov/report)
- Thank you for participating in the weekly SOC call! Your suggestions, comments, and ideas are important to us. We rely on the feedback that we receive from attendees to refine and improve future Technical Exchanges.