GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

27 April 2026

Advisory 140: CISCO - FIRESTARTER Backdoor (CVE-2025-20333) & (CVE-2025-20362).

Release Date: 23rd April 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

These advisory covers two critical vulnerabilities in Cisco's network security products — Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software — that have been actively exploited together by a sophisticated, state-sponsored Advanced Persistent Threat (APT) actor known as UAT-4356 (also tracked as ArcaneDoor and Storm-1849).

What makes this campaign exceptionally dangerous is a second stage: even after organisations patch the two CVEs, a custom-built backdoor called FIRESTARTER may already be embedded in the device. Patching alone does not remove it. The threat actor can continue to access the compromised device indefinitely unless specific additional steps are taken.

What are the systems affected?

The vulnerability affects;

1. **Cisco ASA Platforms**
   - Cisco ASA Hardware Appliances (all models)
   - ASA Service Module (ASA-SM)
   - ASA Virtual (ASAv)
   - ASA firmware on Firepower 2100 / 4100 / 9300
2. **Cisco Firepower and Secure Firewall Platforms**
   - Firepower 1000 Series
   - Firepower 2100 Series
   - Firepower 4100 Series
   - Firepower 9300 Series
   - Secure Firewall 200 Series
   - Secure Firewall 1200 Series
   - Secure Firewall 3100 Series
   - Secure Firewall 4200 Series
   - Secure Firewall 6100 Series
   - Cisco FTD (Firepower Threat Defense) Software

What does this mean?

1. **CVE-2025-20362 – Authentication Bypass:** The attacker sends unauthenticated HTTP/HTTPS requests to restricted URL endpoints on the device's VPN web server. The missing authorization check allows these requests to succeed without any valid credentials.
2. **CVE-2025-20333 – Remote Code Execution:** With access to the restricted endpoints established, the attacker sends specially crafted HTTPS requests that trigger a classic buffer overflow in the VPN web server component. This results in arbitrary code execution on the device, typically with root-level privileges.
3. **LINA Process Injection:** FIRESTARTER reads the memory of the LINA process (the device's core network processing engine) and verifies specific memory patterns to confirm target suitability.
4. **Handler Replacement:** FIRESTARTER overwrites a legitimate WebVPN XML handler function pointer in memory with a pointer to its own malicious Stage 2 shellcode. All incoming WebVPN requests are now intercepted by the attacker.
5. **Magic Byte Trigger:** The malicious handler inspects incoming WebVPN XML request data for a specific custom-defined prefix (magic bytes). When the pattern is matched, the shellcode immediately following it is executed in memory, allowing the attacker to run any command.
6. **Boot Persistence via CSP_MOUNT_LIST:** FIRESTARTER manipulates the Cisco Service Platform mount list (CSP_MOUNT_LIST) so that it is re-executed as part of the device boot sequence. When a graceful reboot or termination signal occurs, FIRESTARTER copies itself to a backup location (/opt/cisco/platform/logs/var/log/svc_samcore.log) and updates the mount list to restore itself on next boot.

7. **Forensic Cleanup:** After each execution, FIRESTARTER restores the original CSP_MOUNT_LIST from a temporary copy, removes itself from disk, and deletes traces — making it appear as though the device is clean during inspection.

Mitigation process

CERTVU recommends the following:

Apply All Required Patches

- **Apply the software updates to address CVE-2025-20333 and CVE-2025-20362** if not already patched
- Apply the recently released Cisco patch specifically created to address the FIRESTARTER persistence mechanism (refer to CISA's Core Dump and Hunt Instructions for device-specific links)
- Apply all subsequent updates via Cisco's download portal within 48 hours of release

Reference

1. https://www.cisa.gov/news-events/directives/v1-ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

.