Multiple Cisco Products Vulnerable to Three Zero-Day Vulnerabilities with Active Exploitation

Summary

On 25 September 2025, Cisco released security advisories disclosing three zero-day vulnerabilities affecting multiple Cisco products including: ASA, FTD, IOS, IOS XE, and IOS XR.

The Canadian Centre for Cyber Security (CCCS), UK National Cyber Security Centre (NCSC), and US Cybersecurity and Infrastructure Security Agency (CISA) have identified active exploitation and successful compromise of Cisco ASA devices.

Details

On 25 September 2025, Cisco released security advisories disclosing three zero-day vulnerabilities affecting multiple Cisco products.

1. **CVE-2025-20333** - Critical (9.9):[1] A remote code execution (RCE) vulnerability affecting the Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) software. A remote attacker with valid VPN credentials can exploit this vulnerability by sending crafted HTTP requests to a vulnerable device, enabling RCE with root privileges.
2. **CVE-2025-20362** - Medium (6.5):[2] An authentication bypass vulnerability affecting the ASA and FTD software. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to a targeted web service on a vulnerable device, enabling access to restricted URLs.
3. **CVE-2025-20363** - Critical (9.0):[3] An RCE vulnerability affecting the ASA, FTD, IOS, IOS XE, and IOS XR software. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to a targeted web service on a vulnerable device, enabling RCE with low user privileges.

Notably **CVE-2025-20333** and **CVE-2025-20362** are under active exploitation by an advanced threat actor, with the Canadian Centre for Cyber Security (CCCS) noting attacks have involved the "deployment of highly sophisticated malware". No publicly available proof-of-concept exploit code has currently been observed.

Affected Products

The following versions of Cisco ASA and FTD are affected by **CVE-2025-20333** and **CVE-2025-20362**:

- Cisco ASA software release 9.12 – versions prior to 9.12.4.72
- Cisco ASA software release 9.14 – versions prior to 9.14.4.28
- Cisco ASA software release 9.16 – versions prior to 9.16.4.85

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O

- Cisco ASA software release 9.17 – versions prior to 9.17.1.45
- Cisco ASA software release 9.18 – versions prior to 9.18.4.67
- Cisco ASA software release 9.19 – versions prior to 9.19.1.42
- Cisco ASA software release 9.20 – versions prior to 9.20.4.10
- Cisco ASA software release 9.22 – versions prior to 9.22.2.14
- Cisco ASA software release 9.23 – versions prior to 9.23.1.19
- Cisco FTD software release 7.0 – versions prior to 7.0.8.1
- Cisco FTD software release 7.1 – all versions
- Cisco FTD software release 7.2 – versions prior to 7.2.10.2
- Cisco FTD software release 7.3 – all versions
- Cisco FTD software release 7.4 – versions prior to 7.4.2.4
- Cisco FTD software release 7.6 – versions prior to 7.6.2.1
- Cisco FTD software release 7.7 – versions prior to 7.7.10.1

The following Cisco products are affected by **CVE-2025-20363**:

- Secure Firewall ASA Software and Secure Firewall FTD Software in specific configurations.[4]
- IOS Software if they have the Remote Access SSL VPN feature enabled.[5]
- IOS XE Software if they have the Remote Access SSL VPN feature enabled.[6]
- IOS XR Software (32-bit) if it is running on Cisco ASR 9001 Routers that have the HTTP server enabled.[7]

CyberAlberta Threat Intelligence identified over 150 assets in the province hosting a Cisco ASA product using internet scanning services.

Related Malware

On 25 September 2025, The National Cyber Security Centre (NCSC)–a part of GCHQ–identified two malware components related to the successful exploitation of Cisco ASA 5500-X Series devices: *RayInitiator* and *LINE VIPER*.[8] *RayInitiator* is a persistent multiple stage bootkit that is flashed to the bootloader of a compromised device and can "survive reboots and firmware upgrades." *LINE VIPER* is a user-mode shellcode loader with several loadable modules that facilitate remote tasking via HTTPS or ICMP, data exfiltration, arbitrary command execution, and suppressing syslog messages.[9]

Cisco assess with "high confidence"[10] this activity is related to the same threat actor that conducted the ArcaneDoor campaign that targeted Cisco ASA devices in early 2024.[11] However, NCSC notes this current campaign "demonstrates an increase in actor sophistication and improvement in operational security" with an "emphasis on defence evasion techniques" in comparison with ArcaneDoor.

Assessment

The exploitation of Cisco ASA devices likely occurred for several weeks, if not months, prior to Cisco's vulnerability disclosure on 25 September 2025, however no official timeline has been published. GreyNoise identified a surge in mass-scanning for Cisco ASA devices in late August 2025 and noted this activity often precedes zero-day exploitation.[12] In the 2024 ArcaneDoor campaign targeting Cisco ASA devices, Cisco Talos researchers subsequently identified exploitation almost 3-4 months prior to the vulnerability disclosure and the

[4] https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo18850
[5] https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo35704
[6] https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo35779
[7] https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo49562
[8] https://www.ncsc.gov.uk/news/persistent-malicious-targeting-cisco-devices
[9] https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/RayInitiator-LINE-VIPER/ncsc-mar-rayinitiator-line-viper.pdf
[10] https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks
[11] https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
[12] https://www.greynoise.io/blog/scanning-surge-cisco-asa-devices

release of software patches.[13] This assessment is made with low-confidence and is limited by the lack of publicly-available compromise data.

Recommendations

Full guidance for identifying product versions and steps for remediation and mitigation are provided in Cisco Security's Event Response report.[14]

- Owners of Cisco ASA, FTD, IOS, IOS XE, and IOS XR assets are strongly recommended to apply patches for newly released secure versions of their products.
- If for any reason a patch is currently unable to be applied, the asset owners are advised to temporarily disable IKEv2 and SSL VPN Services until a full investigation of compromise can be completed, and patches can be applied.
- Cisco noted during incident response that they have not observed successful compromise on assets with Secure Boot and Trust Anchors enabled.

Indicators of Compromise (IOCs)

There are extremely limited IOCs to confirm successful compromise at the time of publication.

- Cisco published a detection guide for identifying compromised devices.[15]
- CISA provided instructions for creating memory dumps, collecting artifacts, and hunting on devices.[16]
- CCCS has provided the following guidance for organizations upgrading Cisco ASA 5500-X devices to 9.12.4.72 or 9.14.4.28:
    - "If the `firmware-update.log` file is found on `disk0:` after upgrading to a fixed release, organizations are encouraged to preserve the log file and notify the Cyber Centre using the contact information below. Instructions regarding transfer of the log file will be provided as part of the follow-up engagement." [17]
- NCSC published a Python script and set of YARA rules for the forensic analysis of memory dumps of Cisco ASA devices.[18]

[13] https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
[14] https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks
[15] https://sec.cloudapps.cisco.com/security/center/resources/detection_guide_for_continued_attacks
[16] https://www.cisa.gov/news-events/directives/supplemental-direction-ed-25-03-core-dump-and-hunt-instructions
[17] https://www.cyber.gc.ca/en/alerts-advisories/al25-012-vulnerabilities-impacting-cisco-asa-ftd-devices-cve-2025-20333-cve-2025-20362-cve-2025-20363
[18] https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/RayInitiator-LINE-VIPER/ncsc-mar-rayinitiator-line-viper.pdf