VULNERABILITY ADVISORIES

New Attack Variant Targeting Cisco Secure Firewalls (CVE-2025-20333 & CVE-2025-20362)

TLP:WHITE

Nov 06, 2025

On November 5, 2025, Cisco updated its security advisories regarding two critical vulnerabilities, CVE-2025-20333 and CVE-2025-20362, affecting Secure Firewall Adaptive Security Appliance (ASA) and Threat Defense (FTD) software, warning of a new, active attack variant.

This variant exploits both flaws to cause an unexpected device reload, resulting in a denial of service (DoS) condition on unpatched appliances. Cisco strongly recommends that users apply the released fixed software to prevent system compromise and service interruption.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to these vulnerabilities.

Analysis

The risk to Cisco Secure Firewall platforms is derived from two distinct vulnerabilities in the VPN web server components. The first vulnerability, CVE-2025-20333, is a critical-severity remote code

execution (RCE) flaw resulting from the improper validation of user-supplied input in HTTP(S) requests. The second vulnerability, CVE-2025-20362, is an unauthorized access flaw that also results from improper input validation, allowing unauthenticated attackers to access restricted URL endpoints related to remote access VPN. Both flaws target the firewall's web-facing VPN server.

Exploiting these flaws allows attackers to achieve devastating levels of compromise. The more severe RCE flaw, CVE-2025-20333, can be leveraged by an authenticated, remote attacker with valid VPN credentials to execute arbitrary code as root on the affected device, potentially leading to its complete compromise. The unauthorized access flaw, CVE-2025-20362, enables an unauthenticated attacker to bypass security controls and access restricted VPN URL endpoints, potentially exposing sensitive data or internal configuration details to external threats.

The immediate concern is the new attack variant Cisco detected on November 5, 2025, which targets devices susceptible to both CVEs. This variant is specifically designed to cause the unpatched firewall devices to unexpectedly reload. This action forces the device into a crash cycle, effectively causing a denial of service (DoS) condition. This evolution of the exploit technique moves beyond initial reconnaissance or direct RCE, instead weaponizing the flaws to immediately impact the network's stability and availability.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Upgrade vulnerable Cisco Secure Firewall ASA and FTD software to the fixed releases specified in the Cisco security advisories.

- Monitor firewall logs and system status for unexpected reloads or service interruptions.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	hhs, cisco, cisco 1, thehackernews, thehackernews 1

Alert ID 8a765f50

View Alert

Share Feedback

was this helpful?  | 

Tags CVE-2025-20362, CVE-2025-20333, Cisco

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**