NATIONAL CSIRT-CY

CVE-2025-20333 **30/9/2025**

Cisco ASA Firewall RCE Vulnerability

Executive Summary

CVE-2025-20333 with a CVSS score of 9.9 is one of the recently disclosed security flaws that has been exploited as part of zero-day attacks targeting Cisco ASA Firewall devices.

This vulnerability allows crafted https requests to exploit the system and allow an authenticated remote attacker to execute remote code execution.

Cisco is urging its users to apply the latest patches.

Cisco released new updates for the remediation of this vulnerability. There are no workarounds that address this vulnerability.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/120.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/cve-2025-20333

Solutions

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments