

Date Posted: 2025/09/30

[Vulnerability Alert] Two Major Security Vulnerabilities Exist in Cisco's Firewall Systems (CVE-2025-20333 and CVE-2025-20363)

- Subject: [Vulnerability Alert] Two Major Security Vulnerabilities Exist in Cisco's Firewall Systems (CVE-2025-20333 and CVE-2025-20363)
- Content:
 - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000015
 - [CVE-2025-20333] A major security vulnerability (CVE-2025-20333, CVSS: 9.9) exists in the VPN Web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) and Cisco Secure Firewall Threat Defense (FTD). The vulnerability stems from improper validation of user-supplied HTTP(S) requests by the server. An attacker holding valid VPN user credentials can leverage a specially crafted HTTP request to allow an authenticated remote attacker to execute arbitrary code as root on the affected device.
 - [CVE-2025-20363] A major security vulnerability (CVE-2025-20363, CVSS: 9.0) exists in the Web services of Cisco Secure Firewall Adaptive Security Appliance (ASA), Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software. The vulnerability is due to improper validation of user input in HTTP requests. An attacker can send a specially crafted HTTP request to the Web service of the affected device to execute arbitrary code as root, potentially leading to a denial of service on the affected device.
- Affected Platforms:
 1. It is recommended to check the official websites for versions to determine if they are affected by this vulnerability.
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-as-aftd-webvpn-z5xP8EUB>
 2. It is recommended to check the official websites for versions to determine if they are affected by this vulnerability.
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-Wmfp3h30>
- Recommended Action:
 - Apply the solution released on the official website for patching:
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-as-aftd-webvpn-z5xP8EUB>
- References:
 - <https://www.twcert.org.tw/tw/cp-169-10411-12ff4-1.html>

Computer and Communications Center

Network Systems Group

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250930_02



Last update: **2025/10/01 16:09**