

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Cisco Patches Critical VPN DoS Vulnerability in ASA and FTD

Date of Publication

October 25, 2024

Admiralty Code

A1

TA Number

TA2024412













Summary

First Seen: October 23, 2024

Affected Product: Cisco ASA and FTD, Cisco Secure FMC, Cisco ASA, Cisco FTC

Impact: Cisco patched a DoS vulnerability (CVE-2024-20481) affecting VPN functions in its ASA and Firepower systems after password spray attacks exposed service disruptions. This flaw could exhaust resources, halting VPN services until devices were restarted. Cisco urges users to update systems and monitor for unusual access patterns.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20481	Cisco ASA and FTD Denial-of-Service Vulnerability	Cisco ASA and FTD			
CVE-2024-20424	Cisco Secure FMC Command Injection Vulnerability	Cisco Secure FMC			
CVE-2024-20329	Cisco ASA SSH Remote Command Injection Vulnerability	Cisco ASA			
CVE-2024-20412	Cisco FTC Static Credential Vulnerability	Cisco FTC			

Vulnerability Details

#1

Cisco recently resolved a significant denial-of-service (DoS) vulnerability within its Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software, both of which provide VPN services. The vulnerability, identified as CVE-2024-20481, was discovered during investigations of password spray attacks, a type of brute-force technique used by attackers attempting to compromise accounts by rapidly testing common passwords on multiple accounts.

#2

In this case, the vulnerability affected the Remote Access VPN (RAVPN) function. During password spray attacks, the repeated access attempts would lead to resource exhaustion, ultimately causing the VPN services to stop functioning correctly and leaving the system vulnerable to further attacks. This DoS condition means that Cisco devices would need to be restarted to regain VPN functionality, significantly disrupting secure access for users.

#3

Cisco released patches to address the vulnerability and issued recommendations for users using ASA and FTD devices. Notably, this is not the only critical flaw Cisco has addressed recently, additional vulnerabilities (CVE-2024-20424, CVE-2024-20329, CVE-2024-20412) in Cisco's Firepower and ASA platforms have also received security patches.

#4

This incident highlights significant security concerns for organizations using Cisco's VPN services. Immediate action is recommended to patch systems and monitor for unusual authentication patterns to safeguard against potential exploits.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20481	Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software	cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:* cpe:2.3:a:cisco:firepower_threat_defense_software:*:*:*:*:*	CWE-772

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20424	Cisco Secure Firewall Management Center Software	cpe:2.3:a:cisco:secure_firewall_management_center_software:*:*:*:*:*:*	CWE-78
CVE-2024-20329	Cisco Adaptive Security Appliance Software	cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*	CWE-146
CVE-2024-20412	Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*	CWE-259

Recommendations



Apply Patches: Immediately apply the latest security patches provided by Cisco for affected ASA and FTD devices. Regularly check Cisco's security advisories for updates on vulnerabilities and patches.



Monitor Authentication Requests: Regularly review logs for unusual spikes in authentication attempts. Implement alerting mechanisms to notify administrators of potential brute-force attacks. Establish baseline metrics for normal traffic to identify anomalies quickly.



Check RAVPN Status: To verify the status of the RAVPN service, execute the command: 'firewall# show running-config webvpn | include ^ enable'. If RAVPN is not required, consider disabling it to reduce your attack surface. Regularly review your configurations to ensure that only necessary services are active, enhancing your overall security posture.



Implement Rate Limiting: Configure rate limiting on authentication requests to mitigate the impact of brute-force attacks. Set thresholds that trigger alerts or block IP addresses after a certain number of failed attempts. This can help prevent resource exhaustion and maintain service availability.



Strengthen Password Policies: Enforce strong password policies requiring complex passwords that are difficult to guess. Implement multi-factor authentication (MFA) for an additional layer of security on VPN access. Regularly educate users about password hygiene and the importance of unique passwords.



Potential MITRE ATT&CK TTPs

<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0040</u> Impact	<u>TA0002</u> Execution
<u>TA0001</u> Initial Access	<u>TA0006</u> Credential Access	<u>T1499</u> Endpoint Denial of Service	<u>T1499.003</u> Application Exhaustion Flood
<u>T1078</u> Valid Accounts	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1203</u> Exploitation for Client Execution
<u>T1588</u> Obtain Capabilities	<u>T1110.003</u> Password Spraying	<u>T1110</u> Brute Force	<u>T1588.005</u> Exploits



Patch Links

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-bf-dos-vDZhLqrW>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5>



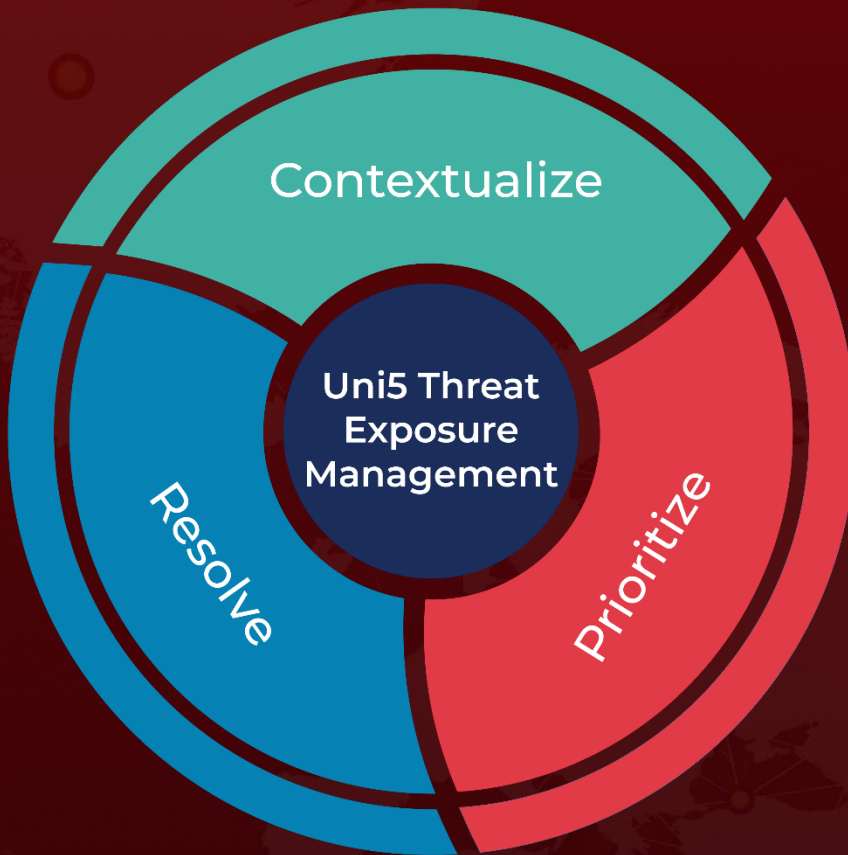
References

<https://www.darkreading.com/application-security/cisco-asa-ftd-software-active-vpn-exploitation>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

October 25, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com