THREAT BULLETINS

Cisco Discloses Max Severity Vulnerability in Firewall Management Center (FMC) (CVE-2025-20265)

TLP:WHITE

Aug 15, 2025

On August 14, 2025, Cisco disclosed a critical remote code execution (RCE) vulnerability, tracked as CVE-2025-20265, affecting Cisco Secure Firewall Management Center (FMC) software.

The flaw has a CVSSv3 score of 10.0 and specifically affects Cisco Secure FMC software versions 7.0.7 and 7.7.0 if they have RADIUS authentication enabled.

Successful exploitation could allow an unauthenticated remote attacker to inject arbitrary shell commands, potentially leading to complete system compromise.

Health-ISAC provides this information to increase situational awareness, encourage users to assess their level of risk to this vulnerability, and apply the available software updates.

The vulnerability, CVE-2025-20265, was disclosed as part of Cisco's August 2025 security advisory bundle and impacts Cisco Secure Firewall Management Center (FMC) software releases 7.0.7 and 7.7.0. It is a command injection flaw caused by a lack of proper user input handling during the authentication phase, and it can only be

exploited if RADIUS authentication is configured for the web-based management interface, SSH management, or both.

A threat actor could exploit this vulnerability by sending specially crafted input while attempting to authenticate through the configured RADIUS server. This malicious input would allow the attacker to bypass the authentication process and inject shell commands that are then executed by the device with high privileges. This is a pre-authentication vulnerability, meaning it can be exploited without any prior knowledge of valid credentials.

The security implications for this vulnerability are critical, given that Cisco FMC is the centralized management platform for an organization's firewalls. A successful compromise of this device would give an attacker a powerful foothold. An attacker with root-level access could disable or modify security policies, reconfigure firewalls to allow malicious traffic, exfiltrate sensitive data, and pivot to other systems on the network.

There were no observations of exploitation in the wild at the time of disclosure. However, organizations using affected products should prioritize the flaw given its maximum severity CVSS score and its pre-authentication remote code execution (RCE) vulnerability status.

Recommendations and Mitigations:

Cisco has released software updates to address CVE-2025-20265. All organizations with affected devices are strongly advised to apply the updates, as this is the primary and most effective solution. If immediate patching is not possible, a temporary workaround is to use another type of authentication, such as local user accounts, external LDAP authentication, or SAML single sign-on (SSO).

Additionally, organizations can further protect their environments via the following:

- Continuously monitoring authentication and system logs for suspicious activity (i.e., failed login attempts or unusual commands)
- Protecting the Cisco FMC management interface with network segmentation to limit public exposure
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	bleepingcomputer, cisco, thehackernews, hhs
Vendors	Cisco

Alert ID 8d710972

View Alert

Share Feedback

was this helpful?  | 

Tags Firewall Management Center, Cisco Secure FMC, CVE-2025-20265, 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/**