Cisco fixed maximum-severity security flaw in Secure Firewall Managemen

Data: 2025-08-15 08:41:35

Autor: Inteligência Against Invaders

Cisco fixed maximum-severity security flaw in Secure Firewall Management Center

Cisco patches critical Secure Firewall Management Center flaw allowing remote code execution on vulnerable systems.

Cisco released security updates to address a maximum-severity security vulnerability, tracked as **CVE-2025-20265** (CVSS score of 10.0), in Secure Firewall Management Center (FMC) Software.

The vulnerability affects the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software.

An unauthenticated, remote attacker can exploit the flaw to execute arbitrary code on affected systems.

The flaw stems from improper input handling during authentication, allowing attackers to send crafted credentials to the configured RADIUS server.

“A vulnerability in the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device.” reads the advisory. *“This vulnerability is due to a lack of proper handling of user input during the authentication phase. An attacker could exploit this vulnerability by sending crafted input when entering credentials that will be authenticated at the configured RADIUS server. A successful exploit could allow the attacker to execute commands at a highprivilege level.”*

Brandon Sakai of Cisco discovered the flaw during internal security testing

The flaw affects Cisco Secure FMC Software versions 7.0.7 and 7.7.0 with RADIUS authentication enabled. ASA and FTD software are not impacted.

The tech giant warns that there is no workaround; however, the flaw is exploitable only if RADIUS authentication is enabled. Mitigation involves switching to local, LDAP, or SAML SSO authentication, after assessing its impact on the specific environment.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of attacks in the wild exploiting this flaw.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,Secure Firewall Management Center)