Vulnerabilitatea Critică de Execuție la Distanță (CVE-2025-20265) în Cisco Secure Firewall Management Center

Introducere	*CVE-2025-20265* este o vulnerabilitate critică în subsistemul *RADIUS* al Cisco Secure Firewall Management Center (FMC) Software. Aceasta permite atacatorilor neautentificați să execute cod arbitrar cu privilegii ridicate pe dispozitivele afectate, compromițând managementul centralizat al infrastructurii de securitate *Cisco*. Vulnerabilitatea a fost descoperită intern de către *Brandon Sakai* de la *Cisco* și a fost făcută publică pe 14 august 2025.
Scor CVSS	10.0 (CRITIC)
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection').
Impact Principal	• Hijacking complet al firewall-urilor: Atacatorii pot prelua controlul asupra *FMC*, permițând modificarea politicilor de securitate, interceptarea traficului sau dezactivarea protecțiilor. • Risc operațional ridicat: Deoarece *FMC* este o componentă centrală în gestionarea firewall-urilor *Cisco*, exploatarea poate afecta întreaga infrastructură securizată,
Mecanism Tehnic și Vectori de Atac	
Cauza Vulnerabilității	Vulnerabilitatea este cauzată de sanitizarea inadecvată a input-ului utilizatorului în timpul fazei de autentificare *RADIUS*. Atunci când *FMC* este configurat să folosească *RADIUS* pentru autentificarea interfețelor web sau *SSH*, metacaracterele shell (de ex., **;**, **|**, **&**) din credențialele introduse nu sunt neutralizate. Acestea sunt transmise către subsistemul de execuție, permițând injectarea de comenzi arbitrare
Condiții pentru Exploatare	Pentru ca un atac să reușească, trebuie îndeplinite trei condiții: • *RADIUS* activat: *FMC* trebuie să folosească *RADIUS* pentru autentificarea interfeței web, *SSH* sau ambele. • Acces la interfețele de management: Atacatorii trebuie să aibă acces la IP-ul public sau intern al *FMC* (porturi *TCP/UDP* relevante pentru web/SSH). • Versiuni vulnerabile: Doar versiunile **7.0.7** și **7.7.0** ale Cisco Secure *FMC* Software sunt afectate. • Condiție: *RADIUS* authentication trebuie să fie activat fie pentru interfața web, fie pentru SSH, fie pentru ambele. • Nu sunt afectate: ✓ Cisco Secure Firewall ASA ✓ Cisco Secure Firewall Threat Defense (FTD)
Analiza Riscurilor și Impact	
Factori de Amplificare a Riscului	• Fără autentificare necesară: Atacatorii nu au nevoie de credențiale valide. • Impact pe întreaga rețea: Datorită permisiunilor ridicate, atacatorii pot compromite nu doar *FMC*, ci și dispozitivele gestionate prin acesta.

<table>
<tr><td></td><td colspan="2">• EPSS (Exploit Prediction Scoring System): Probabilitatea de exploatare în următoarele 30 de zile este estimată la 0.48% (percentila 64%), indicând un pericol iminent,</td></tr>
<tr><td rowspan="4">Consecințe Operaționale</td><td>Tip Impact</td><td>Descriere</td></tr>
<tr><td>Confidențialitate</td><td>Exfiltrarea configurărilor de securitate, politicilor ACL, sau date sensibile.</td></tr>
<tr><td>Integritate</td><td>Modificarea regulilor de firewall, inserare backdoor-uri, falsificare log-uri.</td></tr>
<tr><td>Disponibilitate</td><td>Dezactivarea serviciilor FMC, criptare a datelor pentru ransomware.</td></tr>
<tr><td>Măsuri de remediere</td><td colspan="2">• Actualizarea imediata a aplicațiilor.
• Log-uri de autentificare anormale: Înregistrări cu input-uri ce conțin șiruri de comandă (e.g., rm -rf /, wget payload.sh).
• Procese neobișnuite: Executarea de sh, bash, curl, sau wget de către procesul FMC.
• Modificări neautorizate: Schimbări neexplicate în politicile de securitate sau fișiere de sistem (e.g., /etc/passwd).</td></tr>
<tr><td>Referință</td><td colspan="2">https://securityonline.info/critical-cisco-rce-flaw-cve-2025-20265-cvss-10-unauthenticated-attackers-can-hijack-firewalls/
https://www.cvedetails.com/cve/CVE-2025-20265/
https://zeropath.com/blog/cve-2025-20265-cisco-fmc-command-injection
https://thehackernews.com/2025/08/cisco-warns-of-cvss-100-fmc-radius-flaw.html
https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75415
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79
https://www.criticalpathsecurity.com/urgent-security-advisory-cve-2025-20265-critical-rce-vulnerability-cvss-10-0-in-cisco-secure-fmc/</td></tr>
</table>