AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi Kritike në Cisco Secure Firewall Management Center (FMC) Software

Data: 05/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Së fundi janë identifikuar dy dobësi kritike në softuerin Cisco Secure Firewall Management Center (FMC).

1. Dobësi për Anashkalim të Autentikimit (CVE-2026-20079):

- Lejon një sulmues të paautentikuar dhe në distancë të anashkalojë autentikimin dhe të ekzekutojë skripte arbitrare me privilegje root në sistemin e prekur.

2. Dobësi për Ekzekutim Kodi në Distancë (CVE-2026-20131):

- Lejon një sulmues të paautentikuar dhe në distancë të ekzekutojë kod Java arbitrar si root për shkak të deserializimit të pasigurt në ndërfaqen web.

Të dy dobësitë kanë një **CVSS score 10.0**, që tregon një rrezik kritik. Rekomandohet veprim i menjëhershëm për të reduktuar ekspozimin duke përditësuar në versionet e rregulluara të softuerit.

Informacione Teknike

Detaje të Dobësive:

1. Cisco Secure FMC Authentication Bypass

- **CVE:** CVE-2026-20079
- **CWE:** CWE-288 (Authentication Bypass)
- **Ndikimi:** Akses root në sistemin operativ përmes kërkesave HTTP të manipuluara.
- **Vektori i Sulmit:** Remote, pa autentikim, përmes rrjetit.
- **Mekanizmi:** Një proces i krijuar gabimisht gjatë boot-it të sistemit lejon sulmuesit të anashkalojnë autentikimin dhe të ekzekutojnë skripte.
- **Produktet e prekura:** Cisco Secure FMC Software (on-premises).
- **Nuk preken:**
  - Cloud-delivered FMC (cdFMC)
  - ASA Software
  - FTD Software
  - Security Cloud Control (SCC)

2. Cisco Secure FMC Remote Code Execution (RCE)

- **CVE:** CVE-2026-20131

- **CWE:** CWE-502 (Insecure Deserialization)
- **Ndikimi:** Ekzekutim në distancë i kodit Java arbitrar me privilegje root.
- **Vektori i Sulmit:** Remote, pa autentikim, përmes rrjetit.
- **Mekanizmi:** Deserializimi i pasigurt i objekteve Java të furnizuara nga përdoruesi në ndërfaqen web të menaxhimit lejon përshkallëzim privilegjesh dhe kompromet im të plotë të sistemit.
- **Produktet e prekura:**
  - Cisco Secure FMC Software
  - Security Cloud Control (SCC) Firewall Management
- **Nuk preken:**
  - ASA Software
  - FTD Software

Shënim: Ekspozimi është më i kufizuar nëse ndërfaqja web e FMC nuk është e aksesueshme publikisht.

Rekomandime

AKSK rekomandon:

Përditësim të menjëhershëm i softuerit

- Përditësoni instancat e prekura Cisco FMC në versionet më të fundit të rregulluara sipas advisories të Cisco.

Të kufizoni aksesin në rrjet

- Kufizoni aksesin në ndërfaqen e menaxhimit FMC vetëm për rrjete të brendshme të besuara.
- Implementoni segmentim të rrjetit dhe rregulla firewall për të parandaluar akses publik.

Referenca

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh