Riasztás

Check Point Security Management Server-t érintő sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a Check Point Security Management Servert érintő, CVE-2026-93616 azonosítójú, aktívan kihasznált kritikus sérülékenység kapcsán. A CVSS 9,8-as, előzetes hitelesítés nélkül kihasználható sérülékenység a Check Point Security Management webszolgáltatásában. A hiba directory/path traversal és fájlfeltöltési problémán alapul, amelynek kihasználásával a támadó tetszőleges útvonalról scriptet futtathat, illetve tetszőleges Java class-t tölthet be. Ez a Management Server kompromittálásához vezethet.

A sérülékenység által érintett, illetve javításra szoruló Check Point rendszerek és verziók kerültek azonosításra:

- R82.20 Security Hotfix nélkül
- R82.10 Jumbo Hotfix Take 44 vagy korábbi
- R82 Jumbo Hotfix Take 126 vagy korábbi
- R81.20 Jumbo Hotfix Take 166 vagy korábbi
- R81.10 (EOS) Jumbo Hotfix Take 190 vagy korábbi
- R81 (EOS)
- R80.40 (EOS)
- R80.30 (EOS)
- R80.20 (EOS)
- R80.10 (EOS)
- R80 (EOS)

+36-1-336-4833 csirt@nki.gov.hu

Javasolt intézkedések:

- az érintett rendszereken haladéktalanul telepíteni kell a gyártó által kiadott javítást,
- R82.20 esetén telepíteni kell a Security Hotfixet, illetve a többi érintett verzió esetében a megfelelő javított Jumbo Hotfix Accumulatort,
- a javítás telepítéséig a Management Servereket Security Gateway vagy Check Point tűzfal mögött kell tartani,
- a TCP/19009 porthoz való hozzáférést kizárólag megbízható IP-címekre kell korlátozni,
- a SmartConsole Trusted Clients beállításában kizárólag megbízható, belső IP-címeket kell engedélyezni,
- az összes érintett Management, Logging és SmartEvent szerveren ellenőrizni kell a kompromittálódásra utaló jeleket,
- a cpm.elg naplófájlokban keresni kell szokatlanul hosszú felhasználóneveket,
- ellenőrizni kell a ReflectionUtils-hibákra vonatkozó naplóbejegyzéseket, különösen az allResourceFiles map betöltésének sikertelenségét,
- a naplóbejegyzésekben vizsgálni kell a ../ path traversal-minták előfordulását,
- gyanús találat esetén az érintett rendszert lehetőség szerint izolálni kell, és meg kell őrizni a releváns naplókat és core dumpokat,
- gyanú esetén célzott forensic vizsgálatot kell lefolytatni, és szükség esetén be kell vonni a Check Point Supportot.

A sérülékenység az alábbi, gyártó által kiadott javított verziókra (vagy újabbakra) történő frissítéssel javítható:

- R82.20 Security HotFix Take 1
- R82.10 Jumbo Hotfix Take 45
- R82 Jumbo Hotfix Take 127
- R81.20 Jumbo Hotfix Take 170
- R81.10 Jumbo Hotfix Take 192

Hivatkozások:

https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/
https://cybersecuritynews.com/check-point-management-server-0-day-exploited/

https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-84375

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu