Riasztás Check Point peremvédelmi eszközök sebezhetőségéről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki a Check Point Spark Firewall és Quantum Security Gateway peremvédelmi eszközöket érintő, kritikus besorolású sebezhetőséggel kapcsolatban**.

Az eszközöket érintő hiba kihasználása hálózaton keresztül lehetséges, nem szükséges hozzá külön jogosultság vagy felhasználói interakció. Egy támadó a Remote Access és Mobile Access szolgáltatások tanúsítvány-ellenőrzési folyamatában található logikai hibát kihasználva megkerülheti a felhasználói hitelesítést, és **érvényes felhasználói jelszó nélkül is távoli hozzáférésű VPN-kapcsolatot hozhat létre**. **A sebezhetőséget aktívan kihasználják**, ezért az érintett eszközök frissítését haladéktalanul végezzék el.

Érintett konfigurációk

Security Gateway eszközök

- R82.10 Jumbo Hotfix Take 19 vagy korábbi
- R82 Jumbo Hotfix Take 103 vagy korábbi
- R81.20 Jumbo Hotfix Take 141 vagy korábbi
- R81.10 (EOS)
- R81 (EOS)
- R80.40 (EOS)

Spark Firewall eszközök:

- R80.20.X (EOS)
- R81.10.X
- R82.00.X

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

Feltételek (mindegyiknek teljesülnie kell):

- A VPN Remote Access vagy a Mobile Access engedélyezve van.
- Az IKEv1 engedélyezve van távoli hozzáféréshez.
- Az átjárók elfogadják a régi Remote Access klienseket.
- Az átjárók nem követelnek meg géptanúsítványt a kapcsolatokhoz.

Támadás azonosítása

Az esetleges kompromittációk azonosításához a Check Point SmartConsole naplóiban keressen olyan VPN-tanúsítvány alapú hitelesítési kísérleteket, amelyek kapcsolatba hozhatók a megfigyelt támadói infrastruktúrával és tanúsítvány-alanynevekkel (subject names).

Javasolt időintervallum

Legalább a következő időszakot vizsgálják át: 2026.05.07. – 2026.06.05.

Megjegyzés: A nagyobb biztonság érdekében javasolt az elmúlt 60 nap naplóinak átvizsgálása.

Támadói IP-címek keresése

A SmartConsole-ban navigáljon a Logs & Monitor / Logs & Events menüpontra, majd keressen olyan eseményeket, amelyeknél a forrás- vagy cél-IP-cím megegyezik valamely ismert támadói IP-címmel.

Támadói IP-címek:

- 45.77.149.152
- 209.182.225.136
- 38.60.157.139
- 162.33.177.101
- 45.76.26.42
- 144.208.127.155
- 38.54.88.201
- 38.54.107.167
- 66.42.99.200

- 45.63.104.106
- 45.61.136.173

SmartConsole lekérdezés:

(src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR dst:38.54.107.167 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

Kifejezetten VPN/IKE tevékenység keresése

A találatok azonosítását követően összpontosítsanak a VPN- és IKE-kapcsolódó eseményekre, különös tekintettel a Key Install eseményekre.

Key Install eseményekre szűkített lekérdezés

SmartConsole lekérdezés:

action:"Key Install" AND (src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR dst:38.54.107.167 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

Quick Mode / IKE lekérdezés

Az alábbi lekérdezéssel azonosíthatók azok az IKE-események, amelyek naplóbejegyzése tartalmazza a „Quick” kifejezést:

A sikeres kihasználáshoz (exploithoz) Quick Mode kulcstelepítés (Key Install) szükséges.

Javítás

A javítás a Security Gateways és Spark Firewall verziókra elérhető, és javasolt az azonnali alkalmazás.

- Security Gateway R82.10 - Jumbo Hotfix Accumulator Take 20 és magasabb
- Security Gateway R82 - Jumbo Hotfix Accumulator Take 104 és magasabb
- Security Gateway R81.20 - Jumbo Hotfix Accumulator Take 142 és magasabb
- Spark Firewall R82.00.X - R82.00.10 Build 998002216 és magasabb
- Spark Firewall R81.10.X - R81.10.17 Build 996004901 és magasabb verziók.

Fontos: Az R80.20.X, R80.40, R81 és R81.10 verziók End of Support (EOS) – ezekre nem érkezik javítás, csak az újabb verziókra. Ezeknél a verziók alternatív védelem: IKEv1 letiltása és IKEv2 kizárólagos használata.

Mitigáció

Amennyiben a frissítés haladéktalan elvégzése nem lehetséges, hajtsák végre a Check Point által javasolt mitigációs lépéseket: https://support.checkpoint.com/results/sk/sk185033#TARGET_ID_2

Amennyiben támadásra utaló jelet talál, vegye fel velünk a kapcsolatot a CSIRT@nki.gov.hu email címen!

Források

https://support.checkpoint.com/results/sk/sk185033

https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-50751/