TLP:CLEAR
Szabadon terjeszthető!

RIASZTÁS F5 BIG-IP ACCESS POLICY MANAGER TERMÉKET ÉRINTŐ SÉRÜLÉKENYSÉGRŐL

Tisztelt Ügyfelünk!

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) riasztást ad ki az **F5 BIG-IP Access Policy Managert** (APM modult) érintő, **aktívan kihasznált kritikus sebezhetőségről**. A nyilvános gyártói és nemzetközi kiberbiztonsági partnerszervezetek jelzése szerint a CVE-2025-53521 (CVSS v4.0 szerint 9,3 súlyosságú) az F5 BIG-IP APM komponensét érinti, és a sérülékenységet a támadók már **aktívan kihasználják**. A **CISA a hibát felvette** a Known Exploited Vulnerabilities katalógusba, az **F5 pedig megerősítette**, hogy az érintett, sérülékeny verziók ellen támadásokat figyeltek meg.

A sebezhetőség akkor használható ki, ha a BIG-IP APM hozzáféréskezelési funkciója egy hálózaton elérhető szolgáltatáshoz van konfigurálva. Ekkor **speciálisan kialakított rosszindulatú forgalom távoli kódfuttatást tehet lehetővé**. A hibát eredetileg szolgáltatásmegtagadási hibaként kezelték, de 2026 márciusában új információk alapján RCE-ként sorolták át. Az F5 hivatalos összefoglalója alapján **a támadás hitelesítés nélkül is végrehajtható**, és az Appliance mode rendszer is érintett.

Az **érintett verziók** a nyilvános források szerint a következők:

- 17.5.0–17.5.1, 17.1.0–17.1.2, 16.1.0–16.1.6 és 15.1.0–15.1.10.

A gyártó által **javított verziók**:

- 17.5.1.3, 17.1.3, 16.1.6.1 és 15.1.10.8, illetve ezeknél újabb kiadások.

A támadási lánc a sérülékeny BIG-IP APM rendszer élő forgalmat kezelő apmd folyamatát érinti. A kompromittáció nyomai között szerepelhetnek a lemezen megjelenő vagy módosuló fájlok, olyan naplóbejegyzések, amelyek arra utalnak, hogy egy helyi felhasználó letiltotta a SELinux védelmi modult, valamint a BIG-IP rendszerből származó gyanús HTTP/S forgalom. Az F5 azt is jelezte, hogy a támadó a sys-eicheck integritásellenőrző működését befolyásoló módosításokat is végrehajthat. A gyártó által közzétett megfigyelések szerint a támadók webshellt is elhelyezhetnek, azonban egyes esetekben az ilyen komponensek csak memóriában működnek, ezért a kompromittáció jelei nem minden esetben maradnak meg egyértelműen a fájlrendszeren. A gyártó IoC-ket is közzétett.

A kapcsolódó frissítési csomagok részletei az **F5 tudásbázis K000156741** oldalon érhetők el.

Javasolt intézkedések

- Amennyiben a rendszer az érintett kiadások valamelyikét használja, javasolt a gyártó által megadott **javított verzióra történő azonnali frissítés**.

- A javítás mellett javasolt **a rendszer kompromittálódásának utólagos vizsgálata** is a gyártó által közzétett IoC-k, a webshell nyomok, a SELinux változások és a sys-eicheck integritásával kapcsolatos eltérések alapján.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833