



Riasztás a NetScaler ADC és NetScaler Gateway termékeket érintő sérülékenységekről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a NetScaler ADC és NetScaler Gateway termékeket érintő CVE-2026-88771 és CVE-2026-88772 azonosítójú, aktívan kihasznált kritikus sérülékenységek kapcsán. A gyártó 2026. szeptember 27-én adott ki biztonsági közleményt, amelyben megerősítette, hogy a hibákat a javítások nyilvánosságra hozatala előtt már kihasználták támadók.

A [CVE-2026-88771](#) (CVSS 9.5) egy hitelesítés nélküli, tetszőleges parancsfuttatást lehetővé tevő hiba, amely minden érintett NetScaler ADC/Gateway telepítést érint alapkonfigurációban is. A [CVE-2026-88772](#) (CVSS 9.5) egy memóriatúlcsordulás, amely távoli kód futtatáshoz vagy DoS-hoz vezethet, és a DTLS-t használó eszközöket érinti. Ez alapértelmezetten bekapcsolt beállítás a VPN virtuális szervereken, így a Gateway-ek nagy valószínűséggel érintettek.

A NetScaler ADC és NetScaler Gateway eszközök jellemzően a vállalati hálózatok peremén üzemelnek, VPN-hozzáférést, terheléelosztást és felhasználói hitelesítést biztosítanak, ezért a rajtuk keresztül szerzett hozzáférés a teljes belső infrastruktúra kompromittálódásához vezethet.

A gyártó közleménye szerint az alábbi, korábban kiadott javítást tartalmazó verziók is az érintett tartományba esnek, ezért újbóli frissítés szükséges. A sérülékenységeket az alábbi kiadások javítják, amelyek telepítése minden érintett számára haladéktalanul javasolt:

- NetScaler ADC és NetScaler Gateway 14.1-73.37 és újabb kiadások
- NetScaler ADC és NetScaler Gateway 13.1-64.23 és újabb kiadások
- NetScaler ADC 14.1-FIPS, 14.1-73.37 FIPS és újabb kiadások
- NetScaler ADC 13.1-FIPS és 13.1-NDcPP, 13.1-37.279 és újabb kiadások





Javasolt intézkedések

A javított verziók telepítése minden érintett rendszeren a lehető legrövidebb időn belül, a kiesés időzítésének megtervezésével. A gyártó a közleményben nem adott meg ideiglenes workaroundot, sem egyedi kompromittálódási indikátorokat (IoC). A kockázat csökkentésének egyetlen módja a frissítés.

Mivel a sérülékenységeket már a javítás nyilvánosságra hozatala előtt is kihasználták, a frissítés önmagában nem zárja ki annak lehetőségét, hogy egy támadó korábban már hozzáférést szerzett. A CISA és a Citrix az alábbi lépéseket javasolja gyanú esetén:

- A NetScaler ADC VPX instancia bizonyítékainak megőrzése (pillanatkép, naplók, technikai támogatási csomag, core dump).
- Az eszköz hálózati leválasztása (izolálása).
- Minden hitelesítő adat, hozzáférés és tanúsítvány visszavonása, valamint a helyi fióki jelszavak és kulcstitkosítási kulcsok (KEK) cseréje.
- Az eszközhöz kapcsolódó valamennyi szerver és rendszer átvizsgálása a további kompromittálódás jeleit keresve.
- Az eszköz újratelepítése és a firmware legfrissebb verzióra frissítése.
- A NetScaler Management Services felület nyilvános internetről való elérhetőségének megszüntetése, amennyiben az korábban fennállt.

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

Nemzetbiztonsági Szakszolgálat

Nemzeti Kiberbiztonsági Intézet

Telefon: +36-1-336-4833

Incidentsbejelentés: csirt@nki.gov.hu

