TLP:CLEAR
Szabadon terjeszthető!

Riasztás

Fortinet termékeket érintő magas kockázati besorolású sérülékenységekről

(2024. február 09.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) riasztást ad ki az **FortiOS SSL VPN-**t érintő magas kockázati besorolású sérülékenységek kapcsán, azok súlyossága és aktív kihasználása miatt.

A sérülékenységek az alábbi verziókat érintik:

Verzió	**Érintett:**	**Megoldás:**
FortiOS 7.6	Nem érintett	Nem alkalmazandó
FortiOS 7.4	7.4.0 - 7.4.2	Frissítés a 7.4.3-ra vagy magasabb verzióra
FortiOS 7.2	7.2.0 - 7.2.6	Frissítés a 7.2.7 vagy magasabb verzióra
FortiOS 7.0	7.0.0 - 7.0.13	Frissítés a 7.0.14 vagy magasabb verzióra
FortiOS 6.4	6.4.0 - 6.4.14	Frissítés a 6.4.15 vagy újabb verzióra
FortiOS 6.2	6.2.0 - 6.2.15	Frissítés a 6.2.16 vagy újabb verzióra
FortiOS 6.0	6.0 minden verzió	Áttérés egy fix verzióra

CVE-2024-21762 / FG-IR-24-015: (9.6, kritikus) egy olyan out-of-bounds write sebezhetőség a FortiOS-ben, amely lehetővé teszi a hitelesítés nélküli támadók számára, hogy rosszindulatú kéréseken keresztül távoli kódfuttatást (RCE) érjenek el.

CVE-2024-23113 / FG-IR-24-029 (9.8, kritikus) nem hitelesített támadó tetszőleges kód vagy parancsok futtatását teheti lehetővé speciálisan kialakított kéréseken keresztül

CVE-2023-44487 / FG-IR-23-397 (7.5, magas) A FortiOS nem megfelelő tanúsítvány érvényesítési sebezhetősége lehetővé teheti egy hitelesítés nélküli támadó számára a FortiOS eszköz és egy FortiSwitch példány közötti FortiLink kommunikációs csatorna megfejtését és módosítását.

Javasolt intézkedések

A Gyártó a sebezhetőségek felfedezése után azonnal kiadott egy frissítést, mely letölthető a hivatalos frissítési/letöltési portálról. A fennmaradó támogatott verziókhoz a biztonsági frissítés szakaszosan válik elérhetővé. Ezen felül a gyártó kiadott egy a sebezhetőséget áthidaló megoldást is, aminek az alkalmazásáról az alábbi cikkben található részletes leírás. Azon ügyfeleknek, akik már telepítették a kiadott biztonsági frissítést nem szükséges alkalmazniuk a fenti áthidaló megoldást.

Hivatkozások:

- FG-IR-24-015
- FG-IR-24-029
- FG-IR-23-397

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