Riasztás Fortinet VPN- és tűzfaleszközöket érintő aktív kibertámadási tevékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki a Fortinet VPN és tűzfal eszközöket érintő, jelenleg is aktív kibertámadási tevékenységgel kapcsolatban**.

Nyilvánosságra került információk szerint egy **nagyszabású, automatizált támadási kampány zajlik internet felől elérhető Fortinet FortiGate eszközök ellen**. A biztonsági kutatók által „**FortiBleed**” néven azonosított kampány során a támadók korábban kompromittálódott vagy kiszivárgott hitelesítő adatok felhasználásával kísérlik meg a hozzáférést VPN- és webes menedzsmentfelületekhez. A kutatók szerint több mint 30 000 működő hitelesítő adat került nyilvánosságra, amelyek számos szervezet Fortinet eszközeihez biztosíthatnak hozzáférést.

Érintett rendszerek

- Fortinet FortiGate tűzfaleszközök
- Fortinet SSL-VPN szolgáltatások
- Internet felől elérhető FortiGate webes menedzsmentfelületek
- Olyan Fortinet rendszerek, amelyeknél a hitelesítő adatok korábban kompromittálódhattak vagy hosszabb ideje nem kerültek cserére

A rendelkezésre álló információk alapján **a támadók automatizált eszközökkel pásztázzák az interneten elérhető Fortinet eszközöket**, majd ismert vagy korábban kiszivárgott felhasználónév-jelszó párosok segítségével kísérlik meg a bejelentkezést. Sikeres hozzáférés esetén a támadók jogosulatlan hozzáférést szerezhetnek a szervezet peremvédelmi infrastruktúrájához, amely lehetőséget teremthet további rendszerek elérésére, hitelesítő adatok megszerzésére vagy további támadási tevékenység végrehajtására. **A kampány önfenntartó jellegű**, mivel a megszerzett hitelesítő adatok újabb támadások alapjául szolgálnak.

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

A támadók által használt jelszóállomány jelentős részben korábbi Fortinet incidensek során megszerzett hitelesítő adatokat tartalmaz, ezért különösen veszélyeztetettek azok a szervezetek, amelyek korábbi kompromittálódás után nem hajtottak végre teljes körű jelszócserét.

Kockázat és lehetséges hatások

Sikeres kompromittálódás esetén a támadók:

- jogosulatlan hozzáférést szerezhetnek a szervezeti hálózathoz;
- VPN felhasználói hitelesítő adatokat szerezhetnek meg;
- hálózati konfigurációs és biztonsági információkhoz férhetnek hozzá;
- további rendszerek elleni oldalirányú mozgást hajthatnak végre;
- további hozzáféréseket és jogosultságokat szerezhetnek az érintett környezetben;
- érzékeny adatok kiszivárgását idézhetik elő.

Javasolt intézkedések

Az NBSZ NKI javasolja, hogy a Fortinet VPN- vagy tűzfaleszközöket üzemeltető szervezetek haladéktalanul hajtsák végre az alábbi intézkedéseket:

- Adminisztrátori és VPN-fiókok jelszavainak cseréje, különösen akkor, ha azok az elmúlt években nem változtak.
- Többtényezős hitelesítés bevezetése minden adminisztrátori és távoli hozzáférésű fiók esetében.
- Bejelentkezési naplók felülvizsgálata, különös tekintettel a szokatlan időpontban, ismeretlen helyről vagy nem használt fiókokkal történt hozzáférésekre.
- Menedzsmentfelület internet felőli elérésének korlátozása.
- Firmware frissítése a gyártó által kiadott legfrissebb, támogatott verzióra.

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

Források

https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/

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