

**TLP:WHITE**

**Szabadon terjeszthető!**

**Rendkívüli tájékoztató**  
**Palo Alto Network GlobalProtect firewall**  
**nulladik napi sérülékenységevel kapcsolatban**  
(2021. november 11.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki a Palo Alto Network GlobalProtect Firewall **kritikus kockázati besorolású**, nulladik napi (zero-day) sérülékenységevel kapcsolatban, annak súlyossága és az érintett eszközök széleskörű népszerűsége miatt. A [CVE-2021-3064](#) azonosítón nyilvántartott biztonsági hiba a **PAN-OS 8.1.17** előtti verziókat érinti, a gyártói közlemény alapján a *Prisma Accesst* használók nem érintettek.

A sérülékenység abban az esetben használható ki, amennyiben a „*GlobalProtect portal*” távoli menedzsment funkció engedélyezve van az érintett rendszeren, és a támadó hálózati hozzáféréssel rendelkezik az eszközhöz a szolgáltatási (alapértelmezés szerint 443-as) porton keresztül. Ebben az esetben a jogosultsággal nem rendelkező, távoli támadó *root* szintű parancsfuttatási jogosultságot szerezhet. A hivatkozott felület státusza a „*Network/GlobalProtect/Portals/Network/GlobalProtect/Gateways*” menüpont alatt ellenőrizhető.

**Az NBSZ NKI a biztonsági frissítés haladéktalan telepítését javasolja, amely elérhető az automatikus frissítésen keresztül, valamint manuálisan is letölthető a gyártó honlapjáról.**

**Hivatkozások:**

- <https://security.paloaltonetworks.com/CVE-2021-3064>
- <https://www.randori.com/blog/cve-2021-3064/>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3064>
- <https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/>

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

**TLP: WHITE**