TLP:WHITE
Szabadon terjeszthető!

Riasztás

a Windows Print Spooler szolgáltatást érintő zero-day sérülékenységgel kapcsolatban

(2021.07.07.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet riasztást ad ki **a Windows Print Spooler szolgáltatást érintő kritikus kockázati besorolású zero-day sérülékenységgel[1] kapcsolatban.**

A „PrintNightmare" névre keresztelt sérülékenység (CVE-34527) 2021.07.01-én került publikálásra, melynek kihasználásával a támadó rendszergazdai jogosultságot tud magának szerezni. Ezt követően a támadónak lehetősége nyílik, hogy különböző programokat futtasson, az eszközön található adatokat módosítsa, illetve adminisztrátori jogosultsági körrel rendelkező új felhasználókat hozzon létre.

A Microsoft a sérülékenység javítását célzó biztonsági frissítést tett közzé minden Windows verzió számára, beleértve a már nem támogatott Windows 7 operációs rendszert is.

A javítócsomag részét képezi egy védelmi megoldás egy tetszőleges távoli kódfuttatást lehetővé tevő sérülékenységnek (CVE-2021-1675).

Az NBSZ NKI javasolja a biztonsági frissítések azonnali telepítését, így elkerülve az esetleges sérülékenységek kihasználását.

Az NBSZ NKI által kiadott sérülékenység leírás és a Windows Print Spooler szolgáltatást érintő zero-day sérülékenységgel kapcsolatos hivatkozások:

- https://www.theverge.com/2021/7/2/22560435/microsoft-printnightmare-windows-print-spooler-service-vulnerability-exploit-0-day
- https://www.theverge.com/2021/7/6/22565868/microsoft-printnightmare-windows-print-spooler-service-emergency-patch-hotfix

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

[1] https://nki.gov.hu/figyelmeztetesek/serulekenysegek-uj/windows-print-spooler-serulekenysegek/