TLP: WHITE
Szabadon terjeszthető!

Riasztás

„ZeroLogon” sérülékenységgel kapcsolatban

(2020. szeptember 24.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban: NBSZ NKI**) riasztás**t ad ki a **Microsoft Windows Server DC**-t (*Domain Controller*) érintő **kritikus kockázati besorolású** sérülékenysége kapcsán (CVE-2020-1472), annak súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft *Netlogon Remote Protocol* (MS-NRPC) szolgáltatásban lévő nem megfelelő biztonsági korlátozások miatt, a jogosultsággal nem rendelkező távoli támadó, az MS-NRPC szolgáltatás sérülékenységét kihasználva, adminisztrátori hozzáférést szerezhet az érintett szerverhez. A feltárt hiba a CWE-269 sérülékenység csoportba sorolható.

A sérülékenységet 2020. augusztus hónapban a Microsoft által kiadott frissítés javítja.

Érintett szoftverek (beleértve a Server Core szintű telepítéseit):

- Windows Server 2008 R2 for x64-based Systems Service Pack 1,
- Windows Server 2012,
- Windows Server 2012 R2,
- Windows Server 2016,
- Windows Server 2019,
- Windows Server, version 1903 / 1909 / 2004.

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

További hivatkozások:

- https://hothardware.com/news/dangerous-domain-controller-exploit-zerologon
- https://www.zdnet.com/article/zerologon-attack-lets-hackers-take-over-enterprise-networks/
- https://nvd.nist.gov/vuln/detail/CVE-2020-1472
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
- https://cwe.mitre.org/data/definitions/269.html

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