TLP:WHITE
Szabadon terjeszthető!

Riasztás
Microsoft Exchange szervert termékeket érintő sérülékenységekről

(2022. április 11.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **Microsoft Exchange** szoftvereket érintő **kritikus kockázati besorolású sérülékenységek kapcsán**. Intézetünk itthoni ügyfeleinél tapasztalt aktív kihasználás okán végzett vizsgálatot ASR ügyfelei körében a 2021 augusztusában már az NKI weboldalán is közzétett Microsoft Exchange sérülékenységgel kapcsolatban. A vizsgálathoz használt automata sérülékenységvizsgáló rendszer jelzése szerint az Önök levelező szervere még sebezhető az alábbi sérülékenységek tekintetében.

Microsoft Exchange ProxyShell sebezhetőségekről adott ki 2021. augusztusban riasztást az Egyesült Államok Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége (CISA), a három sérülékenység.

CVE	Risk Rating	Access Vector	Exploitability	Ease of Attack
CVE-2021-34473	High	Network	Functional	Easy
CVE-2021-34523	Low	Local	Functional	Easy
CVE-2021-31207	Medium	Network	Functional	Easy

A Microsoft 2021-ben adott ki javítást a CVE-2021-34473, CVE-2021-34523 és a CVE-2021-31207 azonosítójú sebezhetőségek befoltozására.

Érintett szoftverek:

- Exchange Server 2013 (Cumulative Update 23 and below)
- Exchange Server 2016 (Cumulative Update 20 and below)
- Exchange Server 2019 (Cumulative Update 9 and below)

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítésen keresztül, valamint manuálisan is letölthetőek a gyártói honlapokról.

Az alábbi hivatkozások közül a Mandiant elemzésében található információk alapján ellenőrizhető, hogy történt-e a hivatkozott sérülékenységek kihasználására irányuló támadás az Önök rendszere ellen.

Hivatkozások:

- https://www.securityweek.com/cisa-warns-organizations-proxyshell-attacks-exchange-servers
- https://www.securityweek.com/white-hats-earn-440000-hacking-microsoft-products-first-day-pwn2own-2021
- https://twitter.com/KyleHanslovan/status/1428804893423382532
- https://nki.gov.hu/it-biztonsag/hirek/proxyshell-serulekenysegekrol-adott-ki-riasztast-a-cisa/
- https://www.mandiant.com/resources/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers
- https://advantage.mandiant.com/cve/vulnerability--8e100992-6111-54ed-96b4-f817cf47edd0

TLP:WHITE
Szabadon terjeszthető!

- https://advantage.mandiant.com/cve/vulnerability--f8db969d-dddf-5b2e-81ce-439289be6cde
- https://advantage.mandiant.com/cve/vulnerability--5c5c0f7e-96a8-5403-8487-373322342c46

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