**TLP: WHITE**
**Szabadon terjeszthető!**

# Riasztás
## Microsoft Exchange Szerverek sérülékenységeivel kapcsolatban
(2021. március 03.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztás**t Microsoft **Exchange** valamennyi helyi telepítésű verzióját érintő **soron kívüli hibajavításáról**. A hibajavítás négy, támadók által aktívan kihasznált zero day sebezhetőséget foltoz be. A hibák kihasználásához a támadónak először a 443-as porton keresztül kell hozzáfernie a megcélzott Exchange szerverhez. Amennyiben ez sikeres volt, a négy hiba (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) együttes kihasználásával a támadó teljes kontrollt nyerhet az érintett a szerver felett, azaz a teljes e-mail forgalomhoz hozzáférhet, vagy tetszőleges kód telepítésével a hálózaton tovább is terjeszkedhet. A Microsoft az aktív kihasználásokat a kínai Hafnium APT csoporthoz köti.

Az Microsoft érintett termékei:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

**Az NBSZ NKI a hibajavítás mielőbbi telepítését javasolja Exchange adminisztrátorok számára, amelyről bővebb információ a Microsoft Exchange Team blogján[1] található.**

Az Exchange szerver esetleges **kompromittálódásának ellenőrzéséhez** a Microsoft indikátorokat is nyilvánosságra hozott[2].

**Kapcsolódó hivatkozások:**

[1] https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
[2] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

- https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-bug-this-year/
- https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/
- https://www.bleepingcomputer.com/news/security/sonicwall-releases-additional-update-for-sma-100-vulnerability/

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