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

# Rendkívüli tájékoztató

## Ransomware/Malware terjesztés a Log4Shell sérülékenység kihasználásával kapcsolatban

(2021. december 15.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki a **Log4Shell** sérülékenység kihasználását követő **ransomware**, illetve **egyéb káros kódok** telepítésével kapcsolatban.

2021. december 9.-én ismertté vált „Log4Shell" zero-day sérülékenység (**CVE-2021-44228**) az Apache Log4j Java könyvtárát érinti. A távoli kódfuttatásra módot adó sérülékenység kihasználásával nemzetközi jelzések alapján a támadók többféle (például Khonsari családba tartozó) zsarolóvírust, és más (például **Orcus** elnevezésű távoli hozzáférést biztosító „trójai" malware-t) telepítenek a célrendszerekre.
A verziófrissítés mellett a Log4j csapata számos átmeneti megoldást nyújtó praktikát sorolt fel, amelyek az alábbi hivatkozáson érhetők el: https://logging.apache.org/log4j/2.x/security.html.

A sérülékenység a 2.0-beta9-től a 2.14.1-es verziókig terjed, az **NBSZ NKI** javasolja a mihamarabbi frissítést a legutóbbi, **2.16.0**-ás verzióra, amely a korábbi javítással (**2.15.0**) szemben egy másik – CVE-2021-45046 számon nyilvántartásba vett – szolgáltatás megtagadásos (DoS) támadásra kihasználható sérülékenység ellen is védelmet nyújt.

Az Amerikai Egyesült Államok Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége (CISA) a sérülékenységben érintett szoftvergyártókról és termékekről egy folyamatosan frissen tartott gyűjteményt adott közre, amely innen érhető el: https://github.com/cisagov/log4j-affected-db

**További hivatkozások:**

- https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html
- https://www.bleepingcomputer.com/news/security/new-ransomware-now-being-deployed-in-log4shell-attacks/
- https://success.trendmicro.com/solution/000289946
- https://www.bleepingcomputer.com/news/security/hackers-start-pushing-malware-in-worldwide-log4shell-attacks/
- https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html
- https://nki.gov.hu/it-biztonsag/hirek/log4shell-hirkoveto/

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