Riasztás

Apache Log4j könyvtárt érintő kritikus sérülékenységgel kapcsolatban
(2021. december 11.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztás**t ad ki az **Apache Log4j könyvtár**t érintő **kritikus kockázati besorolású sérülékenységgel kapcsolatban**.

Az Apache Log4j könyvtárt több millió Java alkalmazás használja hibaüzenetek naplózására, melynek sérülékenységét a támadók máris aktívan kihasználják. A CVE-2021-44228, más néven Log4Shell vagy LogJam sérülékenység hitelesítés nélküli, tetszőleges, távoli kódfuttatást tesz lehetővé a támadók számára, melynek sikeres kihasználása estén teljes, rendszerszintű hozzáférést tesz lehetővé.

A probléma kiküszöbölésére az Apache Foundation azt javasolja, hogy mindenki frissítse az érintett könyvtárat a 2.15.0 verzióra, amennyiben ez nem kivitelezhető, használják a következő linken elérhető alternatív megoldásokat:

- https://logging.apache.org/log4j/2.x/security.html

A sérülékenység egyszerű kihasználása végett, az NBSZ NKI a haladéktalan frissítést javasolja!

Hivatkozások:

- https://www.kaspersky.com/blog/log4shell-critical-vulnerability-in-apache-log4j/43124/
- https://www.oracle.com/security-alerts/alert-cve-2021-44228.html

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