HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

EIVOK-22. Szakmai Fórum

Log4j múlt, jelen, jövő

Frész Ferenc Cyber Services, vezérigazgató előadásának rövid összefoglalója.

Az előadó a köszöntés után röviden ismertette szakmai életútját, bemutatta a vállalkozását:
https://cyber.services/
Ismertetésre került, hogy a log4j nem egy új támadási eljárás, több elődje volt pl. a logmérgezés, amely veszélyeire a szakma már 2014-ben felhívta a figyelmet.

A legmagasabb szintű (10) riasztást a log4j-re tavaly év végén adták ki a nemzetközi szervezetek, és ezek alapján az NKI is december 12-én:
https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-apache-log4j-konyvtart-erinto-kritikus-serulekenyseggel-kapcsolatban/

Ezt követően ismertette, a log4j működési mechanizmusát, amely lényege, hogy semmilyen speciális tudást nem igényel a támadó kód bejuttatása egy rendszerbe, elég akár egy webes felületen a felhasználói név helyére beírni, amely esemény naplózásra kerül.
A napló feldolgozását végző rendszerkomponens (parser) feltétel nélkül végre fogja hajtani a támadó utasítását, amely jellemzően egy külső helyről további kód letöltése és futtatása, amely eredménye egy teljes adminisztrátori jogosultság megszerzése a rendszerkomponensekben.

Ezt követően a támadási folyamatot élőben is bemutatta egy oktatói, szeparált/kapszulált rendszerben.
Az log4j érintettségével kapcsolatban felhívta a figyelmet arra, hogy a probléma a közvetlen eseteken túl sokkal nagyobb, mert számos gyártó a rendszereibe beágyazott kódként, a fenyegetettség ismeretének hiányában építette be a sérülékenységet, mint harmadik feles kódot.
Az érintetti körről, valamint a javasolt megoldásokról itt lehet tájékozódni:

https://github.com/cisagov/log4j-affected-db?fbclid=IwAR2WbK-YHZeVig6Irf2SbQeo65MhCJ-9g24fas2WZF3b9v55ddoU_DisCqY

Az előadás végén ismertetésre került, hogy a kódjavításokon, rendszer-frissítéseken, rendszer-hangolásokon túl, --amely a számos egyedi kódfejlesztés miatt évekig is eltarthat-- javasolt a kétirányú hálózati forgalom folyamatos monitorozásával a támadásokat szenzorálni, és a rendelkezésre álló védelmi eszközökkel a forgalomban is a folyamatos védelmet kialakítani.

Az összefoglalót összeállította: Oláh István