Log4J – Mi a legsúlyosabb sérülékenység 2021-ben?

PCLinuxOS Magazine – 2022. január

Írta: Alessandro Ebersol (Agent Smith)

Lezárandó 2021-et, egy komoly sérülékenységet fedeztek fel, ami az egész világot felrázta: a Log4J-hibát.

Az Apple, a Twitter, a Steam és a Tencent cégek által is használt nyílt forráskódú platformban van egy komoly rés, ami lehetővé teszi rosszindulatú egyéneknek érzékeny adatok ellopását, szerverekre fájlok küldését és egyebeket.

A Google szerint több, mint 35 000 Java-csomag érintett, ami azt jelenti, hogy a Maven Central tároló (a fő Java tároló) több mint 8%-át érinti a probléma. A december 16-án felfedezett hiba Jen Easterly, az amerikai Kiberbiztonsági és Infrastruktúrabiztonsági Ügynökség (CISA) vezetője szerint az egyik „legsúlyosabb hiba”, amivel eddig találkozott

Hogyan használhatják ki a támadók a Log4j-hibát?

A Tenable, kibernetikai kutatásra szakosodott cég szerint a Log4J-hiba azért tekinthető kritikusnak, mert a kihasználása viszonylag egyszerű. A sérülés lehetővé teszi azonosítatlan külső támadónak, hogy megtámadja a népszerű Apache Log4J-könyvtárat, amit a cikk elején is említettek mellett számos népszerű szolgáltatás, mint az iCloud, az Amazon és a Tesla is használ.

A Tenable szerint a sérülékenységet kihasználandó a támadó különféle szolgáltatásokon keresztül, mint a Lightweight Directory Access Protocol, Secure (LDAP), a Remote Method Invocation (RMI), és a Domain Name Service (DNS), egy Java Name and Directory Interface (JNDI) injekciót tartalmazó manipulált kérést küldhet.

Magam is néztem pár videót a sérülékenységről és úgy működik, mint egy SQL-injekció, ahol lehetőség van űrlapba parancsot csomagolni.

Amennyiben a sérülékeny szerver Log4J naplókéréseket használ, a sebezhetőséget kihasználó a JNDI-n keresztül rosszindulatú csomagot küld a fent említett szolgáltatások egyikének, mindezt a távoli támadó irányítása mellett.

Mi a Log4J-hiba veszélye?

Amit Yoran, a Tenable kiberbiztonsági szakértője és a igazgatója szerint ez az utóbbi évtized legkritikusabb problémája. Sőt, továbbmenve állítja, hogy a modern számítástechnika történetének legjelentősebb sérülékenysége.

„Ez a fajta sérülékenység arra figyelmeztet, hogy a szervezeteknek fejlett kiberbiztonsági programokat kell kidolgozniuk a dinamikus világ veszélyeire válaszolandó. Noha a részletek még csak szivárognak, arra ösztönözzük a szervezeteket, hogy úgy frissítsék a biztonsági rendszereiket, mintha megsérültek volna, és indítsák be a válaszadásra kidolgozott cselekvési terveket” – jegyzi meg.

Yoran szerint a szervezetekben prioritást kell kapnia a biztonsági és információs feladatokkal foglalkozó csoportokkal való együttműködésnek, hogy megfelelő választ adhassanak a lehetséges incidensekre és meghatározhassák a sérülés belső hatásait.

A legnagyobb veszély, amivel a cégek szembesülhetnek, hogy zsarolóprogram-támadás áldozatai lehetnek. Az ilyen típusú csalás során, a támadó titkosíthatja az áldozat információit. Ezután a számítógépes bűnöző pénzt kér (általában kriptovalutában) az adatok visszaszolgáltatásáért.

Aggódjanak-e a felhasználók?

A legutóbbi javítócsomagok a Log4j-sérülést már megszüntették (Log4j frissítések: 2.3.1 (Java 6), 2.12.3 (Java 7), vagy 2.17.0 (Java 8 és utáni)). Mindazonáltal, a probléma kiterjedt voltára és az érintett cégek nagy számára tekintettel, kell-e a végfelhasználónak aggódnia miatta?

Biztonsági szakértők figyelmeztetnek, hogy a számítógépekre és egyéb személyi eszközökre telepített

alkalmazások ritkán használják a szoftvert, ami nem jelenti, hogy biztonságban lennének. Ellenkezőleg.

Emellett rámutat arra, hogy a személyes adataink különféle szolgáltatók és cégek „kezében vannak”, amik a nyílt forráskódú platformot használják, így a veszély mindenkit érint. Egészségesebb digitális szokásokat kell kialakítani.

A PCLinuxOS tárolójában nincsenek Log4J-t használó alkalmazások. Ez leginkább a szerver-alkalmazásokat célozza, tehát a szerverek sokkal sérülékenyebbek és a cégek általában régebbi, nem frissített Debian szerver-verziókat használnak, és ezeknek a cégeknek a szerverei (és klienseik adatai) ki vannak téve a hibának.