Java turvaauku Log4Shell kasutavad ära lunaraha väljapressijad ja krüptokaevurid, parandus on juba leitud

4 aastat tagasi - 18.12.2021 Autor: AM

Mõned päevad tagasi avastatud ohtlik Java turvaauk Log4j teegis on puudutanud paljusid veebimajutuse teenusepakkujaid ning isegi suuri pilveteenuseid, kuid nüüdseks on peale esimest ebaõnnestunud turvalappi teine turvaparandus olemas, mis peaks ohu serverites kõrvaldama.

Java logimiseks kasutatav kood on kasutusel paljudes tuntud pilveteenustes nagu Apple iCloud, Amazon, Twitter, Cloudflare, Minecraft, samuti mõnedes Eesti e-riigi teenustes. Teada on, et mitmed botnetid nagu Mirai, Tsunami ja Kinsing on juba skännimas netti, et leida haavatavaid servereid lappimata Log4j koodiga ning haavatavatesse Log4Shell turvaauguga serveritesse on istutatud nii krüptokaevandamise kui väljapressimise pahavara.

Apache log4j 2 logimissüsteemile välja antud esimene turvaparandus ilmus küll üsna kohe, kuid hiljem selgus, et uuendus ei tööta kõigi seadistustega. Praeguseks on välja tulnud juba teine turvaparandus.

Sophose turvatarkvaraettevõte pani üles ka mõned "meepotid" (*Honeypot*), mille ainsaks eesmärgiks ongi eksponeerida turvaauguga serverit ja registreerida rünnakud sellele. Alates 9. detsembrist, kui turvaoht avalikuks sai, on "meepoti" ümber tiirelnud tihe ründajate armee, seega turvaauguga serverid, mis on Internetist ligipääsetavad (nii HTTP kui HTTPS-iga), on suures ohus.

Ühe lihtsa testi, kas server on Log4Shell turvaohuga, leiab Huntressilt.

Turvaohu vastu saab, uuendades logimisteegi kiiresti Log4j 2.16 versioonile (või uuemale). Viga esineb ka suurte ja tuntud tehnoloogiaettevõtete toodetes ja teenustes (VMware, Cisco, IBM jt, vt siit), seega nende kasutamisel tuleb ka nende tarkvara kiiresti uuendada.

Microsofti pilveteenuste kaitse kohta saab uusimaid teateid siit.

Google´i pilveteenuste ja soovituste kohta saab lugeda siit.

Lõpetuseks küsimus: keda see puudutab ja kas võib juhtuda, et ka mina olen mõne haavatava teenuse kasutaja? Vastus on karm - kuna tegemist on väga levinud Java logimise teegiga, siis tõenäoliselt puudutab see kuidagi pea kõiki netikasutajaid. Enamuse jaoks muidugi paikab teenusepakkuja turvaaugu enne ära (loodetavasti), kui midagi tõsist juhtub.

- Uudised

Pilt