RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 13 detsember 2021

Kriitiline turvanõrkus Apache Log4j 2 logimistarkvaras

9. detsembril avaldati Java programmeerimiskeele logimistarkvaras Log4j kriitiline turvanõrkus (CVE-2021-44228), mida ära kasutades saab ründaja ligipääsu serverile ning saata sinna pahatahtlikku koodi, paigaldada pahavara ning võtta kontroll serveri üle. Turvanõrkuse tõsidus on rahvusvahelise standardi järgi hinnatud **kõrgeimaks võimalikuks** (10 punkti 10-st) ning see mõjutab maailmas miljoneid seadmeid ja servereid. Kõik tootjad ei ole veel jõudnud turvapaiku välja töötada ja avaldada.

Mõju Eestis

Turvanõrkus mõjutab Eestit otseselt, kuna väga paljud meil laialt kasutusel olevad teenused (F-secure, VMware, erinevad pilveteenused sh Apple iCloud, Amazoni rakendused jne) kasutavad ülal nimetatud logimistarkvara. Nendes kõikides ei pruugi turvanõrkus avalduda, ent potentsiaalselt on haavatavad siiski kümned tuhanded seadmed ja rakendused, mis kasutavad vabavaralise Apache Log4j mitmeid versioone. Turvanõrkus avaldati alles 4 päeva tagasi ning tarkvara- ja seadmetootjad töötavad jätkuvalt välja turvapaiku.

13.12 lõuna seisuga turvanõrkuse massilist ärakasutamist Eestis veel ei ole täheldatud, ent küberkurjategijad kogu maailmas seiravad aktiivselt süsteeme antud nõrkuse suhtes ning otsivad võimalusi sisse tungida. CERT-EE on seni tuvastanud kümmekond ohvrit, kelle hulgas on riigiasutusi ja kohalikke omavalitsusi. Neid kõiki on teavitatud.

Eestis nähtud rünnete tulemusel on peamiselt paigaldatud pahavara, mis hakkab võrgus krüptoraha kaevandama. Potentsiaalselt saab nõrkuse kaudu paigaldada ka lunavara (vastavaid teateid maailmast juba on), varastada andmeid jne. Info nii haavatavuse ärakasutamise ulatuse kui ka rünnete tagajärgede kohta täieneb ajas, selle **potentsiaalne mõju Eestis on väga suur.**

Soovitused infoturbejuhtidele

1. Tuvastada, kas teie asutuse seadmed ja teenused on CVE-2021-44228 kaudu haavatavad (praegustel andmetel puudutab nõrkus Apache Log4j versioone 2.0 – 2.14.1.).

2. Oma Javas arendatud teenuste puhul uuendada viivitamatult Apache Log4j tarkvara uusimale versioonile Log4j 2.15.0 (see versioon tuli välja 9.12).

[1] 1 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

3. Väliste teenusepakkujate puhul jälgida välja antavaid turvauuendusi ning rakendada need esimesel võimalusel. Paljudel teenusepakkujatel, nt F-Secure, on tänaseks paigad olemas ning see info täieneb iga päevaga.

4. Kuna esmajoones on ohustatud teenused, mis on interneti kaudu ligipääsetavad, kaaluda, kas ajutise meetmena (kuni paigatud versiooni tulekuni) on võimalik ligipääsu neile teenustele piirata (need internetist eemaldada, kui risk süsteemi üle võtmiseks on hinnatud suureks). Samuti võib olla abi, kui piirata tulemüüridest haavatavate serverite internetti pöördumist.

5. Jälgida tavapärasest tähelepanelikumalt anomaaliaid oma võrkudes, mis võivad viidata autoriseerimata ligipääsule. Kahtluse korral teavitada cert@cert.ee või https://raport.cert.ee/

RIA väljapoole suunatud tegevused

1. RIA kriitilise informatsiooni infrastruktuuri kaitse osakond teavitas riigiasutusi ja ETO-sid turvanõrkusest 10.12 õhtul e-posti teel (teavitus turvajuhtide ning ETO-de listidesse) ning saatis 11.12 täienduse koos soovitustega;

2. Riigi e-teenustes võeti 10.12 õhtul kasutusele rida ajutisi meetmeid ohu leevendamiseks või paigaldati Log4j versioon, kus mainitud haavatavust pole;

3. CERT-EE teavitas turvanõrkusest 11.12 hommikul oma igapäevases uudiskirjas;

4. RIA kommunikatsiooniosakond teavitas 11.12 avalikkust kriitilisest turvanõrkusest, uudis leidis laia kajastust Eesti meedias.

5. RIA analüüsi- ja ennetusosakond käsitles turvanõrkust 13.12 avaldatud nädalaülevaates.

Rohkem infot:

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

Pidevalt täienev nimekiri tarkvaradest ja teenustest, mida see haavatavus puudutab:

https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592