RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 7. aprill 2022

Kriitilised turvanõrkused Java Spring raamistikus

Taust

Märtsi lõpus avalikustati Java Spring raamistikuga seotud nullpäeva turvanõrkus. Spring on avaliku lähtekoodiga Java raamistik, mille kasutamine lihtsustab ja kiirendab Java programeerimiskeelt kasutavate rakenduste arendamist. Seetõttu kasutavad tarkvaraarendajad üle maailma seda laialdaselt. Microsofti hinnangul on tegu kõige ulatuslikumalt kasutatava avatud lähtekoodiga Java raamistikuga[2].

Turvanõrkust hakati kutsuma nimega **Spring4Shell**. Nimi sarnaneb ülesehituselt eelmise aasta detsembris palju kajastatud kriitilise turvanõrkusega **Log4Shell**, millest kirjutasime samuti[3]. Sarnaselt **Log4Shell** turvanõrkusele on **Spring4Shell kriitiline**, kuna võimaldab eduka ärakasutamise korral lisada haavatavasse serverisse veebikesta (*web shell*). Selle abil on võimalik anda kompromiteeritud süsteemile täiendavaid käske pahaloomulise tegevuse laiendamiseks. Näiteks on ründajal võimalik potentsiaalselt üritada omandada suuremaid õiguseid kompromiteeritud süsteemis või laadida ülesse pahavara, mida saaks kasutada lunavararünnaku sooritamiseks või süsteemis peituvate andmete varastamiseks.

Lisaks **Spring4Shellile** (CVE-2022-22965) väärivad tähelepanu veel kaks Springi raamistikuga seotud turvanõrkust **CVE-2022-22963** ja **CVE-2022-22950**. Esimest nõrkust nimetusega **CVE-2022-22963** hinnatakse **kriitiliseks**, sest see võimaldab autentimata kasutajal samuti koodi kaugkäitust. Teist turvanõrkust nimetusega **CVE-2022-22950** hinnatakse madalama skooriga, kuid seda saab kasutada Spring raamistiku ja Spring Boot komponentide vastu teenusetõkestusrünnete sooritamiseks.

Kuna need turvanõrkused avalikustati alles eelmisel nädalal, siis tegelevad erinevad ettevõtted ja eksperdid üle maailma aktiivselt nende turvanõrkuste analüüsimise, mõju hindamise ja paikade väljastamisega.

Mõju Eestis

Spring raamistiku kasutamine on arendajate seas kogu maailmas üsna levinud. Paratamatult võivad need turvanõrkused avaldada **potentsiaalselt suurt ohtu** ka erinevate organisatsioonide süsteemidele Eestis. 5. aprillil avaldatud uurimuse kohaselt on seni valitud sihtmärgiks kõige enam tarkvaratööstusega seotud ettevõtteid[4]. Siiski tuleks igal organisatsioonil valdkonnast olenemata veenduda, et nende süsteemid ei oleks haavatavad mainitud turvanõrkuste vastu.

---

[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.

[2] https://www.microsoft.com/security/blog/2022/04/04/springshell-rce-vulnerability-guidance-for-protecting-against-and-detecting-cve-2022-22965/

[3] https://www.ria.ee/sites/default/files/content-editors/kuberturve/2021_12_ohuhinnang_apache_log4j.pdf

[4] https://blog.checkpoint.com/2022/04/05/16-of-organizations-worldwide-impacted-by-spring4shell-zero-day-vulnerability-exploitation-attempts-since-outbreak/

Riigi Infosüsteemi Ameti intsidentide käsitlemise osakond (CERT-EE) märkas alates 31. märtsist katseid neid turvanõrkuseid ära kasutada. Arvestades turvanõrkuste kriitilisust ja juba avalikult kättesaadavaid skripte, peab iga organisatsioon arvestama sellega, et kurjategijad kaardistavad aktiivselt haavatavaid süsteeme. Kui leitakse sellised süsteemid, järgneb sellele suure tõenäosusega ka varem või hiljem nõrkuste ärakasutamine.

CERT-EEle ei ole **6. aprilli** seisuga laekunud ühtegi teavitust, et neid turvanõrkusi oleks suudetud edukalt ära kasutada, kuid CERT-EE jälgib pingsalt olukorda ja edasisi arenguid.

Turvanõrkused ja kuidas need paigata

1) Nõrkus: CVE-2022-22965/Spring4Shell (Kriitilisuse skoor **9.8/10**)

Võimaldab autentimata kasutajal koodi kaugkäitust sihtmärgiks valitud haavatavas süsteemis. Turvanõrkuse abil on võimalik kompromiteeritud süsteemi lisada veebikest (*web shell*), mida saab kasutada täiendavate käskude edastamiseks. Lisainformatsiooni turvanõrkuse kohta leiate siit:
https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

Soovitused: Kui kasutusel on Spring 5.3.x -> uuendada versioonile 5.3.18.
Kui kasutusel on Spring 5.2.x -> uuendada versioonile 5.2.20.

Kui uuendamine ei ole mingil põhjusel võimalik, tuleks jälgida lehel toodud alternatiivseid soovitusi.

2) Nõrkus: CVE-2022-22963 (Kriitilisuse skoor **9.8/10**)

Võimaldab autentimata kasutajal koodi kaugkäitust Spring Cloudi komponendi puhul.
Soovitus: Uuendada Spring Cloud Function versioonile **3.1.7** või **3.2.3**.

Lisainfo: https://spring.io/blog/2022/03/29/cve-report-published-for-spring-cloud-function

3) Nõrkus: CVE-2022-22950 (Kriitilisuse skoor **5.4/10**)

Spring Framework ja Spring Boot komponentide teenusetõkestusrünnet võimaldav nõrkus.

Soovitused: Uuenda Spring raamistik vähemalt versioonile 5.3.17. Spring Boot tuleks uuendada versioonini 2.5.11 või 2.6.5.
Lisainfo: https://spring.io/blog/2022/03/28/cve-report-published-for-spring-framework

Soovitused infoturbejuhtidele

1. Tuvastada, kas teie ettevõtte süsteemid on haavatavad ohuhinnangus kajastatud turvanõrkuste vastu. Samuti tuleks veenduda, et teie ettevõtte partnerid, kellel on ligipääs teie süsteemidele, ei oleks haavatavad nende turvanõrkuste vastu. Halbade asjaolude kokkulangemisel võib partneri kompromiteeritud süsteem(id) mõjutada ka teie süsteemi(e).

2. Uuendada haavatavad rakenduste komponendid viivitamatult versioonidele, mille puhul ei ole võimalik turvanõrkuste ärakasutamine või kasutada alternatiivsed meetmeid ohu vähendamiseks.

Uuendamisprotsess võib eeldada muudatusi rakenduste koodis ja rakenduste ümberkompileerimist. Kui see ei ole võimalik, siis soovitame uurida alternatiivseid lahendusi. Näiteks **Spring4Shelli** turvanõrkuse puhul on alternatiivsete kaitsemeetmete rakendamine võimalik (vt siit).

3. Rakendada veebirakenduse tulemüüris (WAFi) vajalikud reeglid, et tõkestada pahaloomulisi päringud. Kui veebirakenduse tulemüüri ei ole seni kasutatud, soovitame seda võimalusel kaaluda, kuna see on kasulik turbemeede kahtlaste päringute tuvastamiseks ja blokeerimiseks.

4. Kuna esmajoones on ohustatud haavatavad teenused, mis on interneti kaudu ligipääsetavad, siis tuleks vajadusel hinnata, kas on võimalik ajutise meetmena (kuni paigatud versiooni või alternatiivsete lahenduste rakendamiseni) ligipääsu neile teenustele piirata (need internetist eemaldada, kui risk süsteemi ülevõtmiseks on hinnatud suureks).

5. Jälgida tavapärasest tähelepanelikumalt anomaaliaid oma võrkudes, eriti neid, mis võivad viidata autoriseerimata ligipääsule. Soovitame lisaks logide ja haavatavate süsteemide uurimisele jälgida ajutiselt ka juba paigatud süsteeme kompromiteerimistunnuste suhtes. Kahtluse korral teavitada cert@cert.ee või https://raport.cert.ee/

6. Kui te ei ole seda veel teinud, soovitame liituda CERT-EE igahommikuse uudiskirjaga, mis toob teieni kõik olulisemad turvanõrkustega seotud uudised. Juhendi, kuidas uudiskirjaga liituda, leiate siit: https://www.ria.ee/et/kuberturvalisus/cert-ee.html

RIA tegevused

1. RIA teavitas 1. aprillil riigiasutusi ja ETO-sid/OTO-sid turvanõrkustest ja võimalikest vastumeetmetest.

2. RIA kaardistab aktiivselt enda teenuste puhul võimalikke haavatavaid komponente ja tegeleb vajadusel turbemeetmete rakendamisega. Lisaks sellele suhtleb RIA enda partneritega, kogub neilt operatiivset tagasisidet ja nõustab neid vajadusel.

3. RIA analüüsi- ja ennetusosakond käsitles turvanõrkust 04.04 ilmunud nädalaülevaates.