RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 17. oktoober 2023

Kriitiline turvanõrkus Cisco IOS XE tarkvaral

Lühikirjeldus

Cisco avalikustas 16. oktoobril, et Cisco IOS XE tarkvara veebiliidest (webUI) mõjutab väga kriitiline turvanõrkus (CVE-2023-20198), mida on ettevõtte sõnul juba kuritarvitatud. Lisaks on ka CERT-EE näinud selle turvanõrkuse kuritarvitamist Eesti küberruumis. Ohustatud on eriti need haavatavad Cisco võrguseadmed, mille webUI veebiliidesed on Internetist kättesaadavad. Hetkel ei ole turvanõrkusele turvaparandust saadaval, kuid haavatavuse saab eemaldada alternatiivse lahenduse abil (kirjeldatud all).

Miks on haavatavus kriitiline?

Konkreetne haavatavus on kriitiline (hinnatud maksimaalse kriitilisuse skooriga CVSS **10.0/10.0**), sest see võimaldab ründajal luua mõjutatud süsteemis kõrgendatud õigustega kasutaja, mida saab seejärel kasutada haavatava võrguseadme üle täieliku kontrolli saamiseks. Sealjuures on ründajal võimalik turvanõrkust ära kasutada autentimata.

Kes ja mida peaks tegema?

Ohus on kõik need võrguseadmed, mis kasutavad Cisco IOS XE tarkvara ja millel on veebiliidese funktsioon lubatud. See funktsioon aktiveeritakse *ip http server* või *ip http secure-server* käskude kaudu.

Selleks, et kontrollida, kas HTTP Server funktsioon on süsteemis lubatud, tegutsege järgnevalt:

- Logige süsteemi sisse ja kasutage käsureal käsku *show running-config | include ip http server|secure|active*
- Eelneva käsu abil saab kontrollida, kas *ip http server* või *ip http secure-server* on lubatud.
- Kui jah, siis on ka veebiliidese funktsioon kasutusel ja **seega võguseade haavatav**.

Cisco soovitab klientidel tungivalt HTTP-serveri funktsioon kõigis internetiühendusega süsteemides keelata. HTTP-serveri funktsiooni keelamiseks kasutage globaalses konfiguratsioonirežiimis käsku *no ip http server* või *no ip http secure-server*. Kui kasutusel on nii HTTP-server kui ka HTTPS-server, on HTTP-serveri funktsiooni keelamiseks vaja mõlemat käsku.

[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.

Cisco avaldas enda ohuteates ka järgneva otsustuspuu, mis võib teid aidata:

Kas kasutate IOS XE-d?

- **Ei.** Süsteem ei ole haavatav. Pole vaja reageerida.
- **Jah.** Kas tarkvaral on *ip http server* või *ip http secure-server* kasutusel?
    - **Ei.** Haavatavust ei saa ära kasutada. Pole vaja reageerida
    - **Jah**. Kas kasutate selle võrguseadmel teenuseid, mis nõuavad HTTP/HTTPSi (nt eWLC)?
        - **Ei.** Keelake HTTP-serveri funktsioon (vt eelnevaid nõuandeid, kuidas).
        - **Jah.** Võimaluse korral piirake juurdepääs neile teenustele usaldusväärsetest võrkudest.

NB! Kui olete konfiguratsioonis vajalikud muudatused teinud, soovitab ettevõte veenduda, et need ka seadme taaskävitamisel endiselt alles on. Selleks tuleks kasutada käsku *copy running-configuration startup-configuration*, et jooksev konfiguratsioon peale muudatuste tegemist ka püsivalt salvestada.

Cisco lisas ka enda ohuteatele juurde juhised, kuidas tuvastada, kas seade on juba potentsiaalselt kompromiteeritud või mitte. Juhised leiate siit, alapeatükist *Indicators of Compromise.*

Cisco ohuteade:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga.