



Lunavararünnakud ohustavad VMware'i ESXi servereid

Olukord

Veebruaris on häkkerid asunud väga aktiivselt ära kasutama paikamata VMware'i ESXi² serverite turvanõrkust **CVE-2021-21974**, mille tulemusena on põhjust rääkida lunavararünnete laviinist. Ehkki turvanõrkus avastati kaks aastat tagasi ja sellele on olemas parandus, leidub selle vastu haavatavaid servereid endiselt. 08.02 seisuga on maailmas selliste lunavararünnakute ohvriks tõenäoliselt langenud ligikaudu paar tuhat ESXi süsteemi ja fookuses näib olevat just Euroopa.

08.02 seisuga on CERT-EEle teada üks juhtum, mille puhul tabas üht Eesti ettevõtet arvatavalt selle turvanõrkuse kaudu tehtud lunavararünnak. Kuna VMware ESXi kasutamine on Eestis üsna levinud, võib CERT-EE hinnangul potentsiaalselt ohustatud Eesti ettevõtteid ja organisatsioone olla palju.

Rünnete iseloomustus ja mõju

- Rünnakute sihtmärkideks valitakse avalikud VMware'i ESXi serverid, mis on haavatavad turvanõrkuse **CVE-2021-21974** vastu. Konkreetse turvanõrkuse vastu tuli uuendus välja juba 2021. aasta veebruaris.
- Teadaoleva informatsiooni kohaselt rünnatakse avatud 427 pordi kaudu (seotud SLP teenusega³).
- Turvanõrkuse eduka ära kasutamise korral on ründajatel võimalik haavatav süsteem üle võtta.
- Seni on teada, et ründajad on kompromiteeritud ESXi serveritel krüpteerinud .vmxf, .vmx, .vmdk, .vmsd ja .nvra laiendiga failid ja lisanud süsteemi lunarahanõuded pealkirjadega „ransom.html“ ja „How to Restore Your Files.html“⁴.

Millised süsteemid on rünnete vastu ohus?

Ründaja saab turvanõrkust ära kasutada juhul, kui tal on ligipääs sihtmärgiks valitud süsteemi SLP teenusele (Service Location Protocol) ja süsteem on haavatav just turvanõrkuse **CVE-2021-21974** vastu (ehk viimased kaks aastat uuendamata). Turvaveast on mõjutatud järgnevad VMware ESXi versioonid:

- ESXi 7.x versioonid, mis on vanemad kui ESXi70U1c-17325551.
- ESXi versioonid 6.7.x, mis on vanemad kui ESXi670-202102401-SG.
- ESXi versioonid 6.5.x, mis on vanemad kui ESXi650-202102101-SG.

Turvanõrkusest on pikemalt kirjutatud [siin](#).

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 ESXi abil on võimalik luua ja kasutada mitmeid virtuaalmasinaid.

³ SLP-d (Service Location Protocol) saavad arvutid ja teised seadmed kasutada teenuste leidmiseks kohalikus võrgus.

⁴ <https://www.bleepingcomputer.com/news/security/vmware-warns-admins-to-patch-esxi-servers-disable-openslp-service/>



Soovitused ettevõtetele ja asutustele, kes kasutavad VMware ESXi:

1. Haavatavad on teatud ESXi servereid (vt loetelu ülal). Veenduge, et teie server ei ole haavatav. VMware'i juhendi ESXi versiooni kontrollimiseks leiate [siit](#).
2. **Uuenda esimesel võimalusel ESXi kõige uuemale versioonile.** Täieliku nimekirja erinevatest versioonidest leiate [siit](#).
3. Kontrollige, millised ESXiga seotud teenused on avalikult kättesaadavad ja piirake võimalusel neile ligipääs ainult usaldusväärsetelt IP-aadressidelt (kehtib eriti SLP teenuse puhul). Kui SLP teenuse kasutamise piiramine ei ole võimalik, on mõistlik selle kasutamine võimalusel peatada. VMware'i juhendi SLP teenuse peatamiseks leiate [siit](#).
4. Isegi, kui haavatavat serverit ei tabanud lunavararünnak, tuleks pärast kaitsemeetmete rakendamist see kindlasti üle kontrollida ja veenduda, et sinna ei ole lisatud muud pahavara.
5. Kui kahtlustate, et teid on tabanud lunavararünnak, andke sellest kindlasti teada CERT-EE-le. Seda saate teha, kirjutades cert@cert.ee või täites küberintsidendi teavitusvormi [siin](#). Teatud juhtudel on võimalik krüpteeritud andmed taastada, CERT-EE eksperdid oskavad teile selles osas nõu anda.

Kui soovid olla kursis Eesti küberruumis toimuvaga, jälgi RIA [kuukokkuvõtteid](#) ja [kvartaliülevaateid](#).

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