



OHUHINNANG

12. august 2025

Microsoft Exchange'is avastati suure mõjuga turvaviga

Taust

USA küberturbeamet CISA avaldas 6. augustil [hoiatuse](#) suure mõjuga turvaveast tähisega CVE-2025-53786, mis võimaldab ründajal pilvekeskkonnas õigusi juurde saada. Selle edukaks ära kasutamiseks on vaja saada administraatoriõigused Exchange'i serveris. Haavatavus mõjutab tarkvara versioone Microsoft Exchange Server 2016, Microsoft Exchange Server 2019 ja Microsoft Exchange Server Subscription Edition RTM.

Microsofti sõnul ei ole neil teada, et hetkel oleks kellelgi õnnestunud turvaviga ära kasutada, kuid nii [Microsoft](#) kui ka CISA on soovitanud kasutusele võtta ennetavad leevendavad meetmed. Kuna Microsoft Exchange Serveri haavatavused on varasemalt olnud tihti ründajate sihtmärgiks, on eriti oluline tarkvara kiire uuendamine.

Ka Eestis on Microsoft Exchange'i tarkvara laialdaselt levinud nii riigiasutustes kui eraettevõtetes. CERT-EE andmetel on mõni Exchange'i versioon kasutusel enam kui 200 erineval juhtumil ja hetkel olemasoleva info põhjal on ligi 40 neist nimetatud turvanõrkuse vastu haavatavad.

Soovitused

1. Kui kasutusel on Exchange hybrid¹, siis tuleks üle vaadata Microsofti välja antud [juhised](#) ja kontrollida, kas kasutusel on turvanõrkuse tõttu ohus olev versioon. Vaadake üle, kas teie kasutatava Exchange jaoks on olemas turvauuendused Cumulative Update (CU).
2. Vaadake üle, kas Exchange'i serverile on rakendatud 2025. aasta aprillis avaldatud [turvapaigad](#) ja jälgige Microsofti [juhiseid](#).
3. Kui kasutusel Exchange hybrid, tuleks üle vaadata ka võtmeandmete (keyCredentials) lähtestamise [juhised](#).
4. Käivitada Microsoft Exchange'i [Health Checker](#), et teha kindlaks, kas on vaja edasisi samme.

Lisaks soovitab CISA eemaldada internetist juurdepääsu kõigile neile Exchange'i või SharePointi serveritele, mis on jõudnud toote tööea lõppu. Näiteks SharePoint Server 2013 ja vanemad on sellised, millele enam turvauuendusi ei pakuta. Exchange 2016 ja Exchange 2019 tootetugi lõppeb 14. oktoobril 2025.

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

¹ Exchange'i hübriidjuurutus võimaldab organisatsioonil integreerida oma kohapealse Exchange'i keskkonna internetile avatud Exchange'i versiooniga.