Turvaauk: MicroTiki ruuteritesse murti sisse

2 kuud tagasi - 09.09.2026 Autor: AM

Lõunanaabrite lätlaste poolt loodud ja kogu maailmas ülimalt populaarsed MikroTiki võrguseadmed on sattunud ulatusliku rünnakulaine alla ning ohumärke on märgatud juba ka siinsamas Eestis.

Kriitilised turvaaugud avastas Poola riiklik küberturbeüksus CERT Polska koostöös OpenAI uusimate tehisarumudelitega GPT-5.5-cyber ja GPT-5.6-sol.

Nimetatud tehisarutiim leidis Läti võrguhiiu tarkvarast RouterOS kuus nõrkust, millest kahte omavahel kombineerides saab ründaja seadme üle võtta ilma ühegi paroolita. Teadlased ristisid selle ründeahela tabavalt nimega MikroTrick.

Piltlikult öeldes toimib esimene turvaauk (tähisega CVE-2026-67276) nagu hajameelne valvur: kui SSH-turvaühenduse loomisel peaks süsteem võrdlema tervet digitaalset võtit, siis RouterOS heitis pilgu vaid võtme ühele osale (avalikule moodulile). Ründajal piisas selle osalisest teadmisest, et meisterdada endale suvalisest traadijupist justkui libavõti, mis uksest ikkagi sisse lasi.

Teine nõrkus (CVE-2026-86060) viis asja aga täieliku absurdini. Kui häkker sisestas kasutajanimeks spetsiaalse keelatud sümboliga algava koodijupi, läks süsteem nii segadusse, et ei visanud sissetungijat mitte välja, vaid määras talle automaatselt kõige kõrgemad administraatori õigused.

CERT Polska hoiatas kogukonda otsekoheselt:

> „Viimastel päevadel oleme täheldanud rünnakuid internetist ligipääsetavate RouterOS-i seadmete vastu. Oleme saanud kinnituse, et ründajad kasutavad seda haavatavuste kombinatsiooni seadmete täielikuks ülevõtmiseks, mille SSH-teenus on avalikest võrkudest kättesaadav.“

Lisaks SSH-augu kaudu sisse hiilimisele leiti seadmetest veel kolmaski ohtlik viga (CVE-2026-67277), mis pesitseb kiirustesti (*bandwidth-test*) teenuses. See võimaldab ründajal ilma sisse logimata tuuma andmeid välja nuhkida või seadme korduvalt kokku jooksutada ja taaskäivituma sundida.

Tuli on lahti: ohus ka Eesti ja Läti seadmed

Kuna MikroTik on Lätis asutatud ja siinkandis legendaarne laialt levinud tootja, levis rünnakulaine kiiresti ka Baltikumis. Läti CERT.LV teatas rünnakute järsust sagenemisest kohalike seadmete vastu. Ka RIA küberturbeüksus CERT-EE on juba tuvastanud esimesed rünnatud ja kompromiteeritud ruuterid Eestis.

Globaalne oht on samal ajal üsna suur. Turvaorganisatsiooni The Shadowserver Foundationi seired näitasid, et ainuüksi 5. septembri seisuga rippus maailmas avaliku interneti poole avatud SSH-pordiga üle 122 500 MikroTiki seadme. Igaüks neist, kel tarkvara värskendamata, on ründajatele kerge saak.

> We added MikroTik SSH identification to our daily scans on 2026-09-04, in response to MikroTik's patches https://t.co/VqlBOo0C8G. As discovered by @CERT_Polska_en https://t.co/5SbLuwuZ1L unpatched MikroTiks can be compromised, if device supports remote access using SSH protocol pic.twitter.com/KpWuwYP2Bj
>
> — The Shadowserver Foundation (@Shadowserver) September 6, 2026

Kas ka sinu ruuteris toimetab kutsumata külaline ops?

Kuidas aru saada, kas sinu ruuter teeb juba salaja häkkerite musta tööd? CERT Polska toob välja väga konkreetsed ohumärgid ehk kompromiteerimise indikaatorid (IoC):

- Seadme logidesse tekivad kummalised read: *login failure for user -2 from <ip> via ssh* ja *user <nimi> added by ssh:-2@<ip>*.
- Süsteemi kasutajate nimekirja on tekkinud kutsumata ja täielike õigustega tegelane nimega ops.
- Edukaid rünnakuid on seostatud eelkõige IP-aadressiga 82.192.72.4 ning rünnakukatseid aadressiga 103.102.31.18.

MikroTik reageeris olukorrale kiirelt ja väljastas juba turvapaigad RouterOS versioonidele 7.25beta3, 7.24.2, 7.23.4 ja 6.49.21.

MikroTik märkis oma ametlikus teadaandes:

> „Tegemist on olulise turvauuendusega. Enamik konfiguratsioone ei ole ohus, kuid uuendamine on tungivalt soovitatav. Et anda aega süsteemide uuendamiseks, ei avalda me praegu üksikasjalikku teavet. Tavalistele koduseadmete kasutajatele ei kujuta probleem otsest ohtu,

kuid soovitame siiski kõigil kasutajatel uuendada.“

Uuendatud tarkvara sisaldab nüüd nutikat enesekontrolli: käivitumisel skannitakse seadistusi ja kui leitakse häkkimise jälgi, lülitatakse kahtlased elemendid välja ning seadmele määratakse hoiatusolek (*Flagged*). Samas hoiatavad nii MikroTik kui ka turbeeksperdid, et hoiatuse puudumine ei anna veel sajaprotsendilist garantiid - ruuteri seadistused tasub alati oma silmaga üle vaadata.

Kuidas oma võrk rünnaku eest kaitsta?

Kui Sinu kodus või kontoris teeb tööd MikroTiki seade, ei tasu jääda ootama, kuni häkkerid uksele koputavad. Turvaspetsialistide retsept on lihtne ja konkreetne:

1. **Uuenda tarkvara kohe.** Paigalda viivitamatult RouterOS-i parandatud versioon (7.25beta3, 7.24.2, 7.23.4 või vanema haru puhul 6.49.21).
2. **Keera avalikud uksed lukku.** Kui Sul pole vältimatut vajadust ruuterit interneti poolt hallata, keela avalikust võrgust ligipääs SSH, WWW/WWW-SSL ja kiirustesti (*bandwidth-test*) teenustele või piira need ainult turvalise sisevõrguga.
3. **Kontrolli kasutajaid ja skripte.** Vaata üle seadme kasutajate nimekiri (otsi eriti kasutajat ops) ja veendu, et käsurealt käsk */system/device-mode/print* ei näitaks häireolekut.
4. **Puhas leht kahtluse korral.** Kui kahtlustad, et pahalased on sinu seadmest juba läbi jalutanud, tee ruuterile täielik tehasealgseadistus (*factory reset*), vaheta välja kõik paroolid ja krüptovõtmed ning taasta seadistus puhtast allikast.

- Uudised

- Turvalisus
- Võrguseadmed

Pilt

mikrotik
hAP ax²
Internet
PoE in / out
LAN
2
3
4
5
PWR USR PoE out
Reset
DC
12-28 V