BR²SEC
KIBERDROŠĪBAS PĒTNIECĪBA UN AUDITI

https://br2sec.com/lv/resursi/cve-2026-103903-routeros-winbox-auth-bypass/
19.10.2026

MikroTik RouterOS WinBox dalītās identitātes autorizācijas apiešana un privilēģiju paaugstināšana (CVE-2026-103903)

BR²SEC pētnieku komanda ir atklājusi kritisku nepareizas autorizācijas ievainojamību (CWE-863, CVSS 8.8) MikroTik RouterOS WinBox autentifikācijas plūsmā. Attālināts autentificēts lietotājs ar tikai lasīšanas (read) tiesībām var iesniegt administratora konta vārdu otrajā posmā un iegūt pilnas administratīvās tiesības (full) bez administratora paroles.

Publicēts: 19.10.2026 · 6 min lasīšanai · Rolands Bīrons



Mākslīgā intelekta ģenerēts attēls · BR²SEC

Privātums un sīkdatnes
Mēs izmantojam nepieciešamās sīkdatnes vietnes darbībai un drošībai. Ar jūsu piekrišanu varam izmantot papildu analītikas sīkdatnes, lai uzlabotu vietni. Izvēli varat mainīt jebkurā laikā.
Sīkdatņu politika Privātuma politika

Tīkls	Zema	Zemas	Nav
IETEKMES JOMA S	KONFIDENCIALITĀTE C	INTEGRITĀTE I	PIEEJAMĪBA A
Nemainīga	Augsta	Augsta	Augsta

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`

Skatīt Enki Guard Intel ↗

> Drošības paziņojums (Security Advisory): Šo ievainojamību atklāja **BR²SEC** drošības eksperts **Rolands Bīrons**.

Ievainojamības kopsavilkums

MikroTik **RouterOS** WinBox autentifikācijas plūsmā pierādītā identitāte netiek nemainīgi sasaistīta ar identitāti, kuras autorizācijas politika tiek uzstādīta sesijai. Uzbrucējs ar derīgu zemu tiesību kontu (piemēram, grupā `read`) var veiksmīgi pabeigt pirmo autentifikācijas posmu ar savu paroli, bet otrajā posmā norādīt esoša administratora lietotājvārdu (piemēram, `admin`).

RouterOS pārbauda zemu tiesību lietotāja kriptogrāfisko pierādījumu, bet sesijai piemēro mērķa konta `full` autorizācijas politiku. Tas ļauj attālinātam autentificētam uzbrucējam iegūt pilnu administratīvu WinBox sesiju un pastāvīgi pārvietot savu kontu uz grupu `full`, nezinot administratora paroli.

Skartais produkts un klasifikācija

- Izstrādātājs: MikroTik (SIA Mikrotīkls)
- Produkts: **RouterOS**
- Skartais komponents: WinBox autentifikācija un lietotāju serviss (TCP ports 8291)
- Skartās versijas: Visas RouterOS versijas zem 7.24.4
- Labotās versijas: RouterOS 7.24.5 stable, RouterOS 7.25rc1 testing un jaunākas
- CVE identifikators: `CVE-2026-103903`
- Klasifikācija: `CWE-863` (Incorrect Authorization), `CWE-287` (Improper Authentication)
- CAPEC: `CAPEC-180` (Exploiting Incorrectly Configured Access Control Security Levels), `CAPEC-115` (Authentication Bypass)
- MITRE ATT&CK: `T1078.003` (Valid Accounts: Local Accounts), `T1068` (Exploitation for Privilege Escalation)
- CVSS 3.1 bāzes vērtējums: **8.8** (High) — `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`
- CVSS 4.0 bāzes vērtējums: **8.7** (High) — `CVSS:4.0/AV:N/AC:L/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`

Ietekmes novērtējums

Šī ievainojamība ļaujnāk apiet RouterOS lomu un tiesību dalīšanas modeli (*Role-Based Access Control*).

Privātums un sīkdatnes
Mēs izmantojam nepieciešamās sīkdatnes vietnes darbībai un drošībai. Ar jūsu piekrišanu varam izmantot papildu analītikas sīkdatnes, lai uzlabotu vietni. Izvēli varat mainīt jebkurā laikā.
Sīkdatņu politika Privātuma politika

1. **Pilnīga iekārtas pārņemšana:** Jebkurš lietotājs ar `read` piekļuvi (piemēram, monitorēšanas vai audita konti) var nekavējoties iegūt `full` administratora privilēģijas.

2. **Konfidencialitātes un integritātes zudums:** Ar pilnām tiesībām iespējams eksportēt rezerves kopijas, ielādēt privātās atslēgas, mainīt ugunsmūra un maršrutēšanas tabulas, kā arī ielādēt pielāgotas pakotnes.

3. **Nav nepieciešama administratora parole:** Uzbrukums neizmanto paroles minēšanu vai spēka paņēmienus (*brute-force*), padarot to klusu un tūlītēju.

Novēršana un rekomendācijas

Jaunināt RouterOS uz versiju **7.24.5 (stable)**, **7.25rc1 (testing)** vai jaunāku versiju. Pārbaudēs apstiprināts, ka šajās versijās dalītās identitātes plūsma tiek korekti noraidīta.

Nepieciešama jūsu organizācijas tīkla iekārtu drošības pārbaude? Uzziniet vairāk par BR²SEC ielaušanās testēšanu un tīkla infrastruktūras auditu.

Privātums un sīkdatnes

Mēs izmantojam nepieciešamās sīkdatnes vietnes darbībai un drošībai. Ar jūsu piekrišanu varam izmantot papildu analītikas sīkdatnes, lai uzlabotu vietni. Izvēli varat mainīt jebkurā laikā.

Sīkdatņu politika Privātuma politika