# 6.49.21 [long-term] is released!

**strods** 1 September 3, 2026, 1:33pm

Before an upgrade:

1. Remember to make backup/export files before an upgrade and save them on another storage device;
2. Make sure the device will not lose power during upgrade process;
3. Device has enough free storage space for all RouterOS packages to be downloaded.

**What's new in 6.49.21 (2026-09-03):**

**This is an important security update. Most configurations are not at risk, but upgrading is highly recommended. To give time to update your systems, we are not currently publishing detailed information.**

- btest - improve stability;
- console - improve stability;
- fetch - improve stability of the TFTP client;
- snmp - improve stability of SNMP;
- ssh - refactor SSH internal processes and improved system stability;
- system - improve stability;
- system - updated certificate for Windows executable signing;
- timezone - updated timezone information from "tzdata2026b" release;

To upgrade, click **Check For Updates** under System/Packages menu and select the **stable** Channel in RouterOS configuration interface, or head to our download page: **http://www.mikrotik.com/download**

- Everything went smoothly
- I encountered an issue after the update (please post about the device, configuration, and unexpected symptoms)
- I encountered an issue, but solved it (please post the solution)

If you experience version related issues, then please send supout file from your router to **support@mikrotik.com**. The file must be generated while a router is not working as suspected or after some problem has appeared on the device

**Please keep this forum topic strictly related to this particular RouterOS release.**

**7.23.4 [long-term] is released!**

**Rb750gr3unstable**

**normis** 2 September 3, 2026, 1:42pm

Please note, we are no longer actively working on the v6 branch and it might contain more undiscovered issues. v7 is truly much more hardened in ways that are impossible to do in v6.

Do upgrade to v7 to stay safe.

---

**rextended** 3 September 3, 2026, 1:50pm

Thanks, is clear, of course.

But nothing already know, right?

---

**infabo** 4 September 3, 2026, 1:51pm

My little "hAP lite" did not run stable on v7. 😭

---

**bratislav** 5 September 4, 2026, 8:15am

I presume if you cut off device internet access you would be pretty safe with ROS 6 in foreseeable future... although one should keep in mind that ROS 6 is using old wireless package that could pose some risk regardless of this newest and obscured one...

---

**rextended** 6 September 4, 2026, 3:21pm

Pleas pin and unpin 6.49.20

---

**mrScamp** 7 September 5, 2026, 9:26am

Mikrotik routeros 6.49.21 started misbehaving after upgrade from 6.49.20.
The device acts as L2TP/IPSEC server.
Incoming connections fail to establish, l2tp server silently drops the tunnel after auth.

The device is not flagged according to /system device-mode output.

```
[admin@RouterOS] > /system device-mode print
  mode: enterprise
```

Upd: setting device-mode flagged=no explicitly resolved the issue.

---

**bratislav** 8 September 5, 2026, 10:35am

What I like in ROS 6 is the ability to disable some packages contained in RouterOS bundle, like ppp or hotspot, if I dont need them and to reduce attack possibilities.
Even better solution would be the ability to disable and immediately shutdown and restart any specific services not only for security reasons but also if it hangs for any reason... maybe something to consider in the future...

---

**tdw** 9 September 6, 2026, 10:12pm

> bratislav:
>
> maybe something to consider in the future...

Most unlikely - there is no ongoing development to v6, only critical security bugfixes

---

**bratislav** 10 September 7, 2026, 7:46am

What I meant was to implement in V7, or some futrue version like V8...

---

**infabo** 11 September 7, 2026, 7:49am

> bratislav:

> like ppp or hotspot, if I dont need them and to reduce attack possibilities.

Disable these features in device-mode.

---

**arshanskiyav** 12 September 7, 2026, 7:51am

Thanks, this helped me. After the update, my GRE tunnels between two RB4011s stayed down.

---

**bratislav** 13 September 7, 2026, 9:32am

It is pretty inconvenient and hardly instantaneous or without interruption since it requires power off or device reset...

---

**infabo** 14 September 7, 2026, 9:37am

Disabling packages in v6 did also require a reboot IIRC.

---

**bratislav** 15 September 7, 2026, 9:57am

Yes but not pressing reset or powering of as in V7...
On the other hand I said that even better solution would be to simply enable starting or stopping services as in most other routers...

---

**tdw** 16 September 9, 2026, 11:01am

We have a number of devices still running v6, after upgrading some RB3011 from 6.49.20 to 6.49.21 OpenVPN connections fail to re-establish.

For Mikrotik client to Mikrotik server connections the server has repeated log entries of 'TCP connection established from x.x.x.x' which are followed by ': using encoding - 'AES-128-CBC/SHA1'

For third-party client to Mikrotik server the server has repeated log entries of 'TCP connection established from x.x.x.x' which are followed by 'duplicate packet, dropping' with a huge list of topics 'ovpn,debug,error,l2tp,unknown,unknown,unknown,unknown,unknown,l2tp,info,unknown, debug'

---

**jlgonzalez** 17 September 10, 2026, 6:45am

Hey!

I have a question regarding how to check if the device has been compromised after upgrading.

According to the documentation provided by MikroTik regarding the vulnerability, `flagged` value under `device-mode` should be `false` after making the upgrade (unless the device has been compromised).

However, on a router running the v6 branch, specifically RouterOS v6.49.21, I get the following output:

```
[user@configtest-v6] > /system device-mode print
  mode: enterprise
[user@configtest-v6] >
```

As you can see, there is no reference to `flagged` (or `flagging-enabled`) in the output.The corresponding parameters do exist in the CLI and configuration menus, but they return `nil` (see the following ouput):

```
[user@configtest-v6] > :put [system device-mode get flagged]

[user@configtest-v6] > :put [system device-mode get flagging-enabled]

[user@configtest-v6] > :put [:typeof [system device-mode get flagging-enable
nil

[user@configtest-v6] > :put [:typeof [system device-mode get flagged]]
nil
```

Is this expected behaviour on RouterOS v6 branch? If so, what is the correct way to check the `flagged` status on RouterOS v6?

Thanks for your time!

**pe1chl** 19 September 14, 2026, 1:52pm

When the device has exposed ssh, webfig or winbox to internet, assume it has been compromised.

The device-mode is a v7 feature, but also it is only for positive indication of compromise, not for negative.

---

**rextended** 20 September 15, 2026, 2:47pm

Any ".5" fix on this version?

---

**EdPa** 21 September 21, 2026, 6:51am

**Version 6.49.22 has been released:**

> **6.49.22 [long-term] is released!**
>
> Before an upgrade: Remember to make backup/export files before an upgrade and save them on another storage device; Make sure the device will not lose power during upgrade process; Device has enough free storage space for all RouterOS packages to be downloaded. What's new in 6.49.22 (2026-09-16): system - improve stability (includes CVE-2026-67281); To upgrade, click Check For Updates under System/Packages menu and select the long term Channel in RouterOS configuration interface, or head to…

---

**next page →**