GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

11 September 2026

Advisory 301: MikroTik RouterOS SSH Login Privilege Escalation and Unauthenticated Bandwidth-Test Service Vulnerabilities (CVE-2026-86060 and CVE-2026-67277).

Release Date: 10th September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, Internet Service Providers, and System/Network administrators that operate a MikroTik router or other device running RouterOS. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-86060 and CVE-2026-67277 are two vulnerabilities in MikroTik RouterOS, the operating system used across MikroTik's widely-deployed router and wireless networking hardware. CVE-2026-86060 is a flaw in the SSH login path: a username beginning with prohibited characters allows an attacker with an unauthenticated SSH session to manipulate RouterOS's trusted policy mask and escalate privileges. CVE-2026-67277 is unrelated in mechanism: RouterOS accepts unauthenticated "related" bandwidth-test (btest) connections before primary session authentication completes, allowing an attacker to trigger an integer underflow that discloses kernel memory and can crash and restart the device.

What are the systems affected?

The following version(s) are affected:

- RouterOS 6.0.0 through 6.49.20 - (Affected)
- RouterOS 7.0.0 through 7.23.3, and 7.24 through 7.24.1 - (Affected)

RouterOS 6.49.21 (Long-term), 7.23.4 (Long-term), 7.24.2 (Stable), and 7.25beta3 (Testing) - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **SSH privilege escalation via a crafted username (CVE-2026-86060)**
    - An attacker opens an SSH session to the RouterOS device using a username that begins with prohibited characters, exploiting an argument-handling flaw that lets the crafted username manipulate the trusted RouterOS policy mask and escalate the session's privileges.
2. **Unauthenticated bandwidth-test connection triggers kernel memory disclosure or crash (CVE-2026-67277)**
    - Separately, an attacker sends an unauthenticated "related" btest (bandwidth-test) connection to the device before primary session authentication completes; RouterOS accepts it, and a resulting integer underflow can disclose kernel memory or trigger a kernel restart, denying service.

Attack vectors:

- A network-based attack against any MikroTik RouterOS device with SSH (CVE-2026-86060) or the bandwidth-test service (CVE-2026-67277) reachable from an untrusted network, most critically the public internet.
- No user interaction is required for either vulnerability. Both are listed by MikroTik and CERT Polska as actively exploited in the wild.

Successful exploitation may allow attackers to:

- Escalate privileges over an unauthenticated SSH session and, when chained with the related CVE-2026-67276 authentication bypass, take full administrative control of the device.
- Disclose kernel memory or crash and restart the device via the bandwidth-test service, disrupting network availability without any authentication.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade RouterOS to 6.49.21 (Long-term), 7.23.4 (Long-term), or 7.24.2 (Stable) as applicable, per MikroTik's September 2026 security advisory. A single upgrade resolves both vulnerabilities in this advisory as well as the actively-exploited CVE-2026-67276 chain.

2. Restrict SSH and bandwidth-test exposure to trusted networks

Report any suspected compromise of a MikroTik RouterOS device to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-86060
2. https://www.cve.org/CVERecord?id=CVE-2026-67277
3. https://mikrotik.com/supportsec/september-2026-vulnerability/