An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609070233

# NCSC Advisory

## Critical Vulnerbilities in Mikrotik: RouterOS

CVE-2026-67276, CVE-2026-86060 and CVE-2026-67277

**7th, September 2026**

**STATUS: TLP:CLEAR**

**Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

**For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.**

# Description

CVE ID: CVE-2026-67276

**Published:** 2026-09-05

**Vendor:** Mikrotik

**Product:** RouterOS

**CVSS Score[1]:** 9.2

# Products Affected

| Product | Version |
|---|---|
| RouterOS | 7.24 < 7.24.2 |
| RouterOS | 7.0.0 < 7.23.4 |
| RouterOS | 6.0.0 < 6.49.21 |

# Impact

RouterOS does not compare the complete RSA public key when matching an SSH authentication request to an authorized user key, checking the key type and modulus but omitting the exponent. Because signature verification uses the client-supplied key, an attacker knowing an authorized RSA modulus can supply a key with exponent one, forge a valid signature, and open an SSH command channel as the target user without the private key.This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable),

Common Weakness Enumeration (CWE)[2]: CWE-347: Improper verification of cryptographic signature

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://db.gcve.eu/kev-catalogs

# Description

CVE ID: CVE-2026-86060

**Published:** 2026-09-05

**Vendor:** Mikrotik

**Product:** RouterOS

**CVSS Score:** 9.2

# Products Affected

| Product | Version |
|---|---|
| RouterOS | 7.24 < 7.24.2 |
| RouterOS | 7.0.0 < 7.23.4 |
| RouterOS | 6.0.0 < 6.49.21 |

# Impact

RouterOS contains an argument-handling flaw in the SSH login path involving usernames that begin with a prohibited character, allowing for the trusted RouterOS policy mask to be changed, leading to privilege escalation. Exploitation requires an unauthenticated SSH session to reach the RouterOS login helper.This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable),

Common Weakness Enumeration (CWE): CWE-88: Improper neutralization of argument delimiters in a command ('Argument Injection')

Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: N/A

# Description

CVE ID: CVE-2026-67277

**Published:** 2026-09-05

**Vendor:** Mikrotik

**Product:** RouterOS

**CVSS Score:** 8.8

# Products Affected

| Product | Version |
|---|---|
| RouterOS | 7.24 < 7.24.2 |
| RouterOS | 7.0.0 < 7.23.4 |
| RouterOS | 6.0.0 < 6.49.21 |

# Impact

RouterOS accepts a "related" btest connection before the corresponding primary session has completed authentication. An unauthenticated client can use this state to start an IPv4 UDP test. With "random-data=false", the sender transmits an uninitialized tail from a kernel packet buffer. A separate unchecked, inverted packet-size interval causes unsigned integer underflow, anomalously large fragmented output, and can restart the RouterOS kernel. This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable),

Common Weakness Enumeration (CWE): CWE-306: Missing authentication for critical function

Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: N/A

# Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Mikrotik.

CVE-2026-67276

- https://nvd.nist.gov/vuln/detail/CVE-2026-67276
- https://www.cve.org/CVERecord?id=CVE-2026-67276

CVE-2026-86060

- https://nvd.nist.gov/vuln/detail/CVE-2026-86060
- https://www.cve.org/CVERecord?id=CVE-2026-86060

CVE-2026-67277

- https://nvd.nist.gov/vuln/detail/CVE-2026-67277
- https://www.cve.org/CVERecord?id=CVE-2026-67277

CVE-2026-67276, CVE-2026-86060, CVE-2026-67277

- https://cert.pl/en/posts/2026/09/mikrotik-routeros-cve
- https://cert.pl/en/posts/2026/09/vulnerabilities-in-mikrotik-routeros-actively-exploited/
- https://npratley.net/reversing-mikrotiks-silent-patch-the-routeros-7-23-4-fix-they-wouldnt-explain/
- https://mikrotik.com/supportsec/september-2026-vulnerability/
- https://forum.mikrotik.com/t/6-49-21-long-term-is-released/272802
- https://forum.mikrotik.com/t/7-23-4-long-term-is-released/272801
- https://forum.mikrotik.com/t/7-24-2-stable-is-released/272800