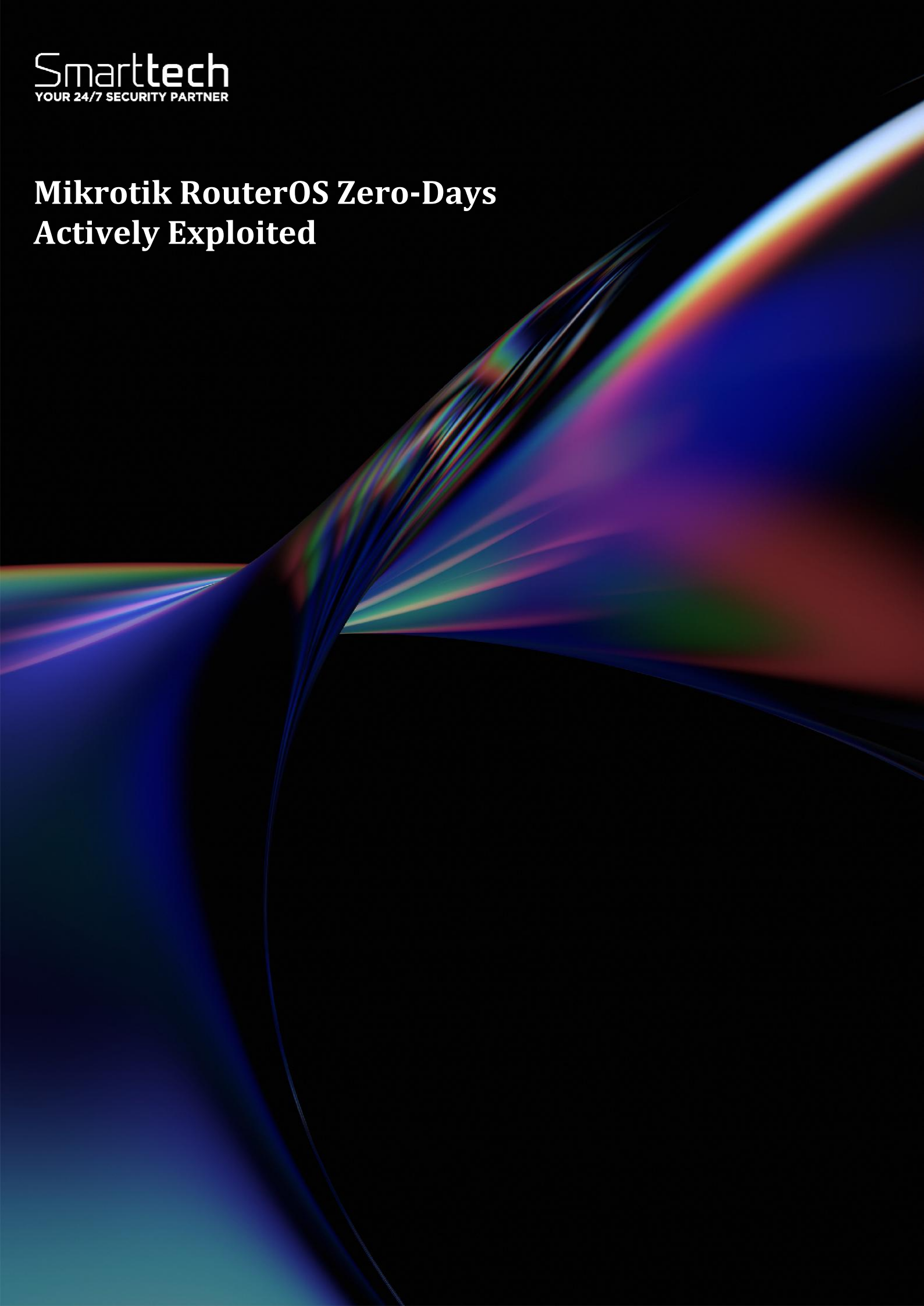
Smarttech
YOUR 24/7 SECURITY PARTNER

Mikrotik RouterOS Zero-Days Actively Exploited



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	153
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-08
Issue Date	2026-09-07

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

New vulnerabilities have been identified in Mikrotik RouterOS that are being actively exploited in the wild. Tracked as CVE-2026-67276, CVE-2026-86060 and CVE-2026 67277, these flaws stem from improper RSA key validation in SSH authentication, an argument-handling flaw in the SSH login process involving usernames beginning with a prohibited character, and an authentication bypass condition involving related btest connections. Successful exploitation could allow unauthorized SSH access, escalate privileges, information disclosure, or cause system instability and kernel restarts.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to this vulnerability are as follows:

CVE ID	Description
CVE-2026-67276 **CVSS Base Score: 9.2**	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).
CVE-2026-86060 **CVSS Base Score: 9.2**	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).

CVE-2026-67277 **CVSS Base Score: 8.8**	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).

Indicators of Compromise (IoCs)

IP addresses:

- 82.192.72.4
- 103.102.31.18

RouterOS log entries:

- login failure for user -2 from <ip> via ssh
- user <name> added by ssh:-2@<ip>

Accounts:

- The existence of a highly privileged account named "ops"

Note: *The absence of the traces mentioned above does not rule out unauthorized activity.*

Affected Products

Product	Affected Version
RouterOS	7.24 < 7.24.2
	7.0.0 < 7.23.4
	6.0.0 < 6.49.21

Recommendations

We recommend the following actions be taken:

- Apply appropriate updates, hot fixes or mitigations provided by Mikrotik to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through

automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. **(M1037: Filter Network Traffic**)
    - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender

Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

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

CVE

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

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com