

Alert Bulletin

Bulletin N.: 97

Publication Date: 07/09/2026

Subject: Alert 2026-97 Zero-day in MikroTik RouterOS actively exploited via SSH exposed to the Internet

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected range	Minimum fixed version
MikroTik RouterOS 6	6.0.0 up to before 6.49.21	6.49.21
MikroTik RouterOS 7 Long-term	7.0.0 up to before 7.23.4	7.23.4; 7.23.5 is recommended for additional regression fix
MikroTik RouterOS 7 Stable	7.24 up to before 7.24.2	7.24.2
MikroTik RouterOS 7 Development	Not listed in the CERT range	7.25beta3

Description

Recently CERT Polska and MikroTik published a security advisory about **six ZeroDay vulnerabilities** in **MikroTik RouterOS**, including flaws that allow SSH authentication bypass, opening unauthenticated SSH channels, arbitrary file reading through WebFig, privilege escalation, TLS certificate spoofing, and denial of service. The publication includes **CVE-2026-67276, CVE-2026-67277, CVE-2026-67278, CVE-2026-67279, CVE-2026-67281, and CVE-2026-6060**, with severities ranging from **High to Critical**.

The vulnerabilities with the highest impact are **CVE-2026-67276**, which allows spoofing SSH authentication of users with authorized RSA keys; **CVE-2026-67279**, which allows opening an SSH channel and executing requests without completing authentication; and **CVE-2026-67281**, which allows reading protected files from the WebFig /jsproxy endpoint, potentially including configurations and credentials stored on the router. The combination of these flaws may allow a remote unauthenticated attacker to gain access to the device, extract sensitive information, modify configuration files, or escalate privileges.

CERT Polska confirmed active exploitation of a two-vulnerability chain, named **MikroTrick**, against MikroTik routers that have SSH accessible from the Internet. Although the manufacturer and CERT have confirmed the activity, the two specific CVEs that make up this chain have not been publicly disclosed; therefore, it is

recommended to consider all RouterOS systems within the vulnerable ranges as priorities for update and compromise review.

The disclosed flaws are as follows:

CVE	Severity / type	Main impact
CVE-2026-67276 (CVSSv4 9.2)	Improper cryptographic validation, CWE-347	Allows spoofing SSH authentication as an authorized user with an RSA key, without possessing the private key.
CVE-2026-67277 (CVSSv4 8.8)	Missing authentication for critical function, CWE-306	Allows initiating unauthenticated IPv4 UDP tests via btest; may leak uninitialized data from the kernel buffer and cause kernel reboots due to a packet size error.
CVE-2026-67278 (CVSSv4 6.3)	Improper cryptographic validation, CWE-347	Allows spoofing certificates during X.509 validation and impersonating TLS servers if the attacker controls or redirects outgoing connections from the router.
CVE-2026-67279 (CVSSv4 6.9)	Improper workflow, CWE-341	Allows opening an SSH session channel without authentication and executing requests that enable creation, overwriting, or rebuilding of files in the managed RouterOS space.
CVE-2026-67281 (CVSSv4 8.7)	Access of uninitialized pointer, CWE-324	Allows unauthenticated reading of files through WebFig /jsproxy, including files owned by root and potentially configuration stores with credentials.
CVE-2026-86060 (CVSSv4 9.2)	Argument injection, CWE-388	Allows altering the RouterOS policy mask and escalating privileges through a weakness in the processing of usernames during SSH login.

Solution

Update RouterOS immediately to a fixed and supported version:

- RouterOS 6: 6.49.21 or later.
- RouterOS 7 Long-term: 7.23.5 or later.
- RouterOS 7 Stable: 7.24.2 or later.

<https://help.mikrotik.com/docs/spaces/ROS/pages/328142/Upgrading+and+installation>

Review the device’s security status after updating via:

/system/device-mode/print

RouterOS may mark the device as Flagged if it detects suspicious configurations during startup checks.

- Review logs and configuration for:
- Unknown local users, especially privileged accounts named ops.
- Account creation events with the ssh:-2@ indicator.

- Unrecognized scripts, *scheduler jobs*, firewall rules, NAT, VPN, proxy, DNS, or tunnels.
- Unexpected files, modified configurations, or administrative changes outside the maintenance window.

Additional recommendations:

- Mantener las reglas de firewall por defecto de MikroTik, que normalmente bloquean la exposición pública de puertos de administración en dispositivos domésticos mientras no hayan sido modificadas.
- Establecer acceso de administración por una red de gestión dedicada, VPN administrativa o *jump host* , en lugar de exponer SSH, WinBox, WebFig o API directamente a Internet.
- Aplicar listas allowed-address para las cuentas administrativas y limitar el acceso a servicios de gestión usando reglas de firewall de entrada.
- Deshabilitar servicios no utilizados, especialmente btest, FTP, Telnet, HTTP, API y APIs legacy.
- Centralizar logs de RouterOS en un servidor remoto/SIEM, de modo que la evidencia permanezca disponible aun cuando el atacante manipule o reinicie el dispositivo.

Regularly validate the configuration through controlled backups and change comparisons; treat unauthorized modifications on perimeter devices as a possible security incident.

Additional information:

- <https://cert.pl/en/posts/2026/09/mikrotik-routeros-cve/>
- <https://thehackernews.com/2026/09/attackers-hijack-mikrotik-routers.html>