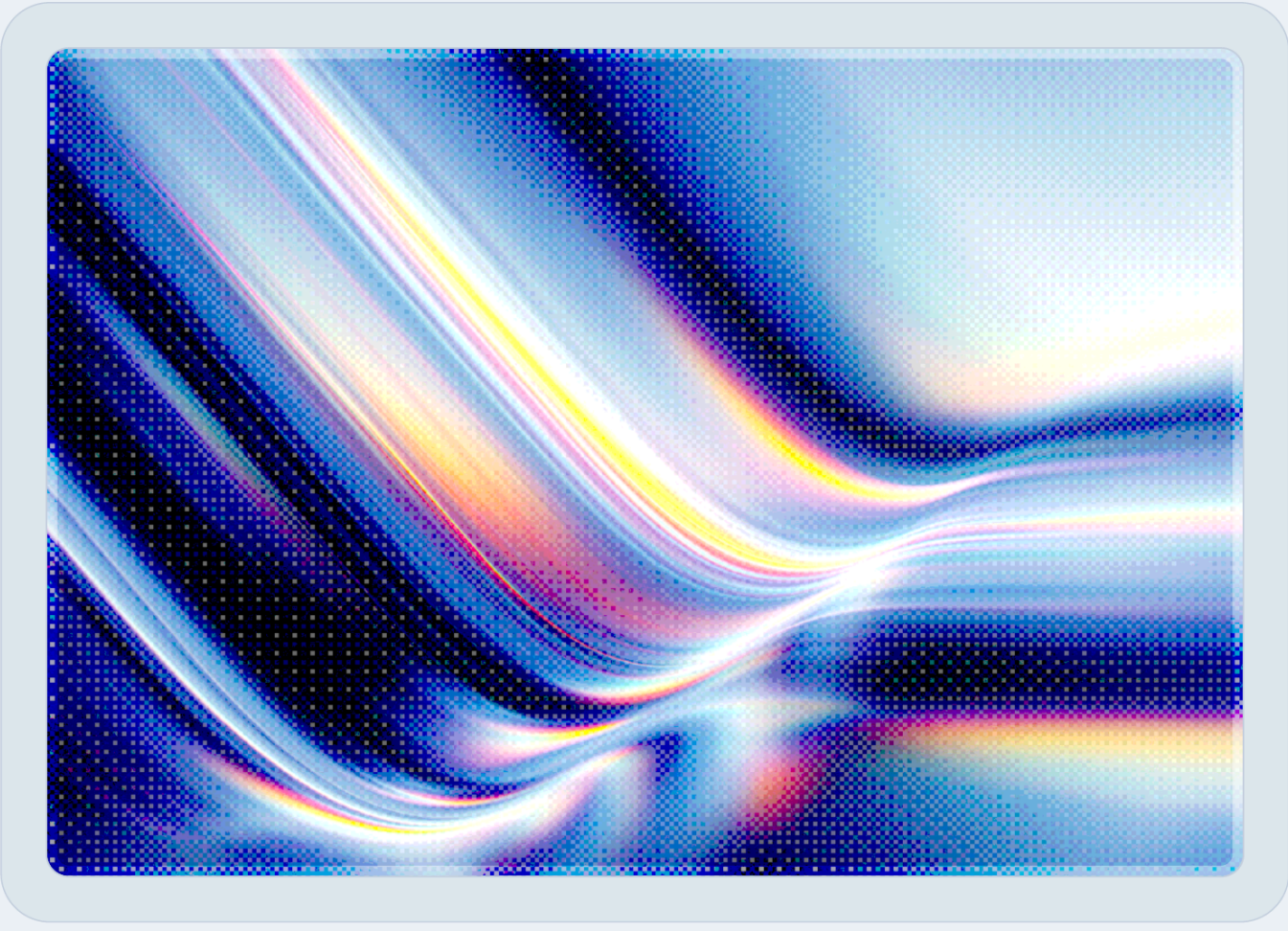
CSAI Foundation | Cloud Security Alliance

MikroTrick: Chained MikroTik RouterOS Flaws Bypass SSH Authentication

2026-09-07

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- CERT Polska, working with MikroTik, disclosed six RouterOS vulnerabilities on September 5, 2026, two of which chain together — under the name "MikroTrick" — to let an attacker with no credentials take full administrative control of a router whose SSH service is reachable from the internet.
- The core flaw, CVE-2026-67276 (CVSS 9.2), stems from RouterOS validating only the key type and modulus of an SSH public key during authentication, not the full key, so an attacker who knows an authorized user's RSA modulus can forge a valid key without ever holding the private key.
- A second flaw, CVE-2026-86060 (CVSS 9.2), lets an attacker who has reached this pre-authentication state escalate to full administrative privileges through a crafted username that RouterOS's SSH login helper misinterprets as a command-line argument.
- Active exploitation was underway by at least September 2, 2026 — a day before MikroTik shipped unannounced patches on September 3 and three days before public disclosure — meaning attackers had a working exploit chain before defenders had a CVE number to search for.
- MikroTik fixed the flaws in RouterOS 6.49.21, 7.23.4, and 7.24.2 (also present in the 7.25beta3 development build); organizations running exposed RouterOS devices should patch immediately and treat any device that was internet-facing during the exposure window as potentially compromised.

Background

MikroTik RouterOS is the operating system underpinning the company's RouterBOARD and cloud router hardware lines, widely deployed by internet service providers, small and mid-sized businesses, and network hobbyists because of its low cost and extensive configurability. That same accessibility has made RouterOS a persistent target: internet-wide scanning research has repeatedly found large populations of MikroTik devices with management interfaces reachable from the public internet, including a 2023 Censys survey that counted nearly 450,000 hosts still exposing vulnerable RouterOS

configuration interfaces months after a prior critical patch [1]. Many of these devices, once installed at a customer site or network edge, receive little ongoing administrative attention, which extends the window during which a newly disclosed flaw remains exploitable in the field long after a fix is available.

On September 5, 2026, CERT Polska published a coordinated disclosure describing six new RouterOS vulnerabilities, three of them critical, discovered through its own research and reported to MikroTik prior to release [2][3]. MikroTik's own advisory, published the same week, was brief on technical detail, noting only that "most configurations are not at risk, but upgrading is highly recommended" [2] — a level of detail that, if consistent with the company's past disclosures, would suggest a deliberate strategy of limiting exploit detail until patch adoption builds, though CSA has not verified this pattern independently. The Hacker News reported that attackers were already abusing the flaw chain against internet-exposed SSH services before the public advisory landed [7]. CERT Polska's own advisory confirmed the exploitation window with server-side telemetry beginning September 2 [4], and independent researcher Costin Raiu, along with Security Affairs and HOL, published corroborating technical accounts of the same activity [5][6]. The combined chain has been given the name "MikroTrick" by researchers tracking the campaign, reflecting how two individually narrow bugs — one in key validation, one in username parsing — combine into a complete pre-authentication takeover.

Security Analysis

The MikroTrick chain is best understood as two failures in RouterOS's SSH implementation that, used together, remove the need for any valid credential. CERT Polska's disclosure also covered four additional issues: a separate SSH connection-protocol flaw that permits an unauthenticated session channel, a bandwidth-test service vulnerability that is itself high-severity (CVE-2026-67277, CVSS 8.8), a signature-validation flaw, and a WebFig information-disclosure issue. All six are summarized alongside the core chain in the table below.

CVE	CVSS	Component	Vulnerability
CVE-2026-67276	9.2	SSH public-key authentication	Validates only RSA key type and modulus, not the exponent, allowing a forged key (e.g., exponent 1) to authenticate as an authorized user without the private key
CVE-2026-86060	9.2	SSH login helper	A username beginning with a disallowed character (e.g., "-2") is passed to a legacy login helper that treats it as a

CVE	CVSS	Component	Vulnerability
			command-line flag, enabling privilege escalation to full administrative access
CVE-2026-67279	6.9	SSH connection protocol	Accepts the post-authentication connection protocol after a client-initiated rekey even when authentication never completed, letting an unauthenticated attacker open a session channel and issue commands that create, overwrite, or reconstruct files — including configuration and diagnostic data — in RouterOS's managed file namespace
CVE-2026-67277	8.8	Bandwidth-test (btest) service	Unauthenticated access to a privileged code path, combined with a memory-disclosure and integer-underflow flaw, enabling information leakage or denial of service
CVE-2026-67278	6.3	RSA/PKCS#1 signature validation	Flawed signature checking could allow an attacker to forge a trusted intermediate certificate for an arbitrary hostname
CVE-2026-67281	8.7	WebFig `/jsproxy`	Uses an uninitialized authorization pointer, potentially exposing root-owned files through the file-serving path

Sources: [3][6][7]

The exploitation mechanics of the primary chain are what distinguish MikroTrick from an ordinary authentication bug. Standard SSH public-key authentication requires an attacker to possess the private key matching a public key already authorized on the target account. RouterOS's implementation, per CERT Polska's analysis, compared an offered key against the authorized key list using only its type and RSA modulus — omitting a check of the public exponent [3][6]. An attacker who already knows (or can guess) the modulus of a legitimately authorized key — plausible where keys are reused across a fleet of devices, published inadvertently, or derived from a weak generation process — can construct an alternative key pair sharing that modulus with an exponent of 1, then forge a valid-looking signature that RouterOS accepts as though the real private key had signed it. Independent lab reproduction reported

that this technique worked reliably against RSA keys generated with a low public exponent, though keys using the more common exponent 65537 were not universally susceptible, suggesting the practical blast radius depends on how authorized keys were originally generated [6].

That authentication bypass alone would grant access only as whatever user's key was forged. CVE-2026-86060 is what turns it into full administrative compromise. RouterOS's SSH login path did not adequately reject usernames beginning with a hyphen, and a value such as "-2" reached a legacy login helper that interprets leading-hyphen arguments as command-line options rather than as a literal username. Chained after the key-validation bypass, this let attackers manipulate the router's internal policy mask and elevate an initial low-privilege foothold to a full administrative session [3][6]. Because both flaws sit in code paths reachable purely through SSH — a service administrators frequently leave open for legitimate remote management — the combination requires no user interaction, no valid password, and no social engineering.

Evidence gathered by CERT Polska and by Raiu indicates the chain was already being used in the wild before either the patch or the advisory existed. RouterOS system logs record failed and successful authentication attempts using the artifact username "-2," visible via the `/system history` log as entries resembling `ssh:-2@<attacker-IP>`, often followed immediately by unauthorized user creation or firewall rule changes [5]. Attack traffic has been traced to at least two source IPs, 82.192.72[.]4 (hosted on a Leaseweb range) and 103.102.31[.]18, with the former also hosting a payload described as a MIPS-architecture BusyBox binary nearly identical to a 2010-era official BusyBox release, alongside supporting Python and shell scripts [5]. That the observed payload reuses over a decade-old, publicly available tooling rather than custom malware suggests the operators prioritized speed and reliability over stealth or sophistication once the access primitive was in hand — consistent with opportunistic, internet-wide scanning rather than a narrowly targeted campaign, though CSA has not independently verified attacker identity or motive.

The timeline compounds the risk. MikroTik shipped fixed builds — 6.49.21, 7.23.4, and 7.24.2 — on September 3, 2026, two days before CERT Polska's public advisory, but exploitation activity had already been observed from at least September 2 [2][5]. That sequencing means a meaningful population of devices was exposed to a working, unauthenticated exploit chain for several days with no public indicator to search for, and it means the population of devices compromised before patching may substantially exceed the population still vulnerable today, though no independent data yet quantifies this comparison. RouterOS includes a "Flagged" status mechanism intended to surface certain compromise indicators at startup, which MikroTik and CERT Polska both point to as a starting point for post-patch triage, though it should not be treated as an exhaustive compromise check given how narrowly it is scoped [2][4].

Recommendations

Immediate Actions

Organizations operating MikroTik RouterOS devices should upgrade to 6.49.21, 7.23.4, or 7.24.2 (or the 7.25beta3 development release, where applicable) without delay, prioritizing any device whose SSH, WinBox, HTTP/S management, or bandwidth-test service has ever been reachable from the public internet. Before and after patching, administrators should review `/system history` and connection logs for the "-2" username artifact or other unexpected login identifiers, and audit the user list for unfamiliar accounts — CERT Polska specifically flagged unauthorized "ops" accounts as an observed post-compromise indicator [3][5]. Any device showing the "Flagged" compromise indicator, unexplained configuration changes, or unrecognized scheduled scripts should be treated as compromised: isolated from the network, its logs preserved for analysis, and restored from a known-good configuration with new credentials and SSH keys rather than simply patched in place [2][4].

Short-Term Mitigations

Where immediate patching is not feasible across an entire fleet, administrators should restrict SSH and other management-plane services to trusted source IP ranges via firewall rules, or disable internet-facing management access entirely in favor of an out-of-band or VPN-based path such as WireGuard, which MikroTik itself recommends as the preferred remote-management transport [2]. Because CVE-2026-67276 depends partly on how authorized keys were generated, organizations should also inventory and, where practical, regenerate SSH keys authorized on RouterOS devices using strong, modern parameters rather than assuming legacy keys are safe by default. Given that the bandwidth-test service (CVE-2026-67277) and WebFig's `/jsproxy` path (CVE-2026-67281) carry their own unauthenticated exposure risks, these should be disabled on any device that does not require them, independent of the SSH chain.

Strategic Considerations

MikroTrick fits a pattern CSA has tracked across recent boundary-device incidents (see CSA Resource Alignment, below), in which internet-facing management interfaces on network and security infrastructure — not just endpoint or application software — become an attractive access vector, plausibly because these devices are often trusted, less closely monitored than servers, and patched less frequently. Organizations should formally elevate edge and perimeter network devices to the same patch-priority tier as internet-facing servers and security appliances, maintain an accurate asset

inventory of RouterOS (and comparable) deployments including firmware version, and apply Zero Trust principles — authenticating and authorizing management-plane access before any network-layer response is returned, rather than exposing SSH or HTTP management services directly to the internet — as a structural mitigation against the next chain of this kind, not just this one.

CSA Resource Alignment

CSA's rapid-research threat advisory on FortiSandbox Triple-CVE: Security Appliances as Network Entry Points analyzes a closely analogous pattern: unauthenticated vulnerabilities in an internet-reachable network appliance being actively chained and exploited within days of disclosure. Its guidance to elevate security and network appliances into the highest patch-priority tier, restrict management-interface exposure to known administrative ranges, and treat these devices as potential pivot points rather than inherently trusted infrastructure applies directly to MikroTrick's exploitation of internet-facing RouterOS SSH services.

CSA's research note on Cisco SD-WAN CVE-2026-20245 Zero-Day: Root Access Pre-Disclosure Exploitation documents the same incident shape as MikroTrick: a network management-plane vulnerability exploited in the wild for months before a public patch existed, ultimately granting attackers persistent, root-level control. Its finding that pre-disclosure exploitation windows on management infrastructure can run far longer than defenders assume reinforces the case for treating patch delay on these devices, not just the initial vulnerability count, as a primary risk driver.

CSA's advisory on CVE-2026-0257: GlobalProtect Authentication Bypass Under Active Exploitation offers a further parallel: another boundary-device authentication bypass exploited within days of patch availability, where the underlying lesson — that cryptographic checks must validate a credential completely, not partially — mirrors RouterOS's incomplete RSA key comparison in CVE-2026-67276. That advisory's recommendation to separate management-plane access from general network access and to restrict exposure by source range is equally applicable here.

CSA's Stealth Mode SDP for Zero Trust Network Infrastructure whitepaper describes the structural alternative to MikroTrick's root cause: an authenticate-before-connect model in which management-plane services are never visible to unauthenticated network traffic at all, closing off the class of attack that this incident and the GlobalProtect, FortiSandbox, and Cisco SD-WAN cases all represent, rather than relying solely on patch velocity after each new chain is found.

Finally, findings should be evaluated against the AI Controls Matrix (AICM) v1.1, whose Threat & Vulnerability Management and Infrastructure & Virtualization Security domains cover patch prioritization for network infrastructure and restriction of administrative interfaces, providing organizations a control

framework against which to assess and document their MikroTrick remediation posture.

References

[1] Censys. "MikroTik RouterOS CVE-2023-30799: On the Dangers of Public Admin Interfaces." Censys Blog, August 2023.

[2] MikroTik. "September 2026 Vulnerability." MikroTik Security Advisories, September 2026.

[3] CERT Polska. "Vulnerabilities in MikroTik RouterOS software." CERT Polska, September 5, 2026.

[4] CERT Polska. "Critical vulnerabilities in MikroTik RouterOS are being actively exploited. Immediate update recommended." CERT Polska, September 5, 2026.

[5] Security Affairs. "Your MikroTik Router May Already Be Compromised: Look for SSH User "-2"." Security Affairs, September 2026.

[6] HOL. "BREAKING: CVE-2026-67276 and MikroTrick can take over MikroTik RouterOS with SSH exposed." HOL Blog, September 2026.

[7] The Hacker News. "Attackers Hijack MikroTik Routers Through Internet-Exposed SSH Without Authentication." The Hacker News, September 2026.