

Alert Bulletin

Bulletin N.: 83

Publication Date: 05/08/2026

Subject: Alert 2026-83 Critical DoS Vulnerability in MikroTik RouterOS

Traffic Light Protocol (TLP): White

Affected product(s):

- MikroTik RouterOS – all versions
- MikroTik Cloud Hosted Router – all versions

Description

CVE-2026-16347 (CVSS 8.8 – High) has been published in MikroTik RouterOS and Cloud Hosted Router: an authentication flaw with no effective rate limiting that allows an attacker to brute-force the administration API until obtaining valid credentials. No patch is available as of the date of publication; ZoomEye identifies more than 934,000 globally exposed instances.

MikroTik RouterOS is the proprietary operating system developed by MikroTik and used in routers, switches, and network devices widely deployed across enterprise environments, ISPs, and critical and industrial infrastructure worldwide. On July 28, 2026, the vulnerability **CVE-2026-16347** (CVSS 4.0: **8.7 / CVSS 3.1: 8.8 – High**) was published, classified as **CWE-307 (Improper Restriction of Excessive Authentication Attempts)**, affecting the authentication handling of the **administration API** of RouterOS and Cloud Hosted Router across **all available versions**. CISA published a specific advisory on this vulnerability, and the ZoomEye team identified more than **934,800 globally exposed instances** searchable using the filter `vul.cve="CVE-2026-16347"` or the dork `app="MikroTik RouterOS"`.

- **CVE-2026-16347 – Improper Restriction of Excessive Authentication Attempts in RouterOS API (CVSS 4.0: 8.7 / CVSS 3.1: 8.8 – High)**

The MikroTik RouterOS API authentication system does not implement effective controls against excessive login attempts. Specifically: `nvd.nist+2`

- There is no significant **rate limiting** for failed authentication attempts.
- There is no **account lockout** mechanism or account blocking after multiple failures.
- No **source IP restrictions** are applied to repeated attempts.
- In some versions there is a **fixed per-connection delay**, but it can be easily bypassed through **concurrent sessions**, allowing a high volume of attempts to be distributed across multiple

As a result, an attacker with network access to the administration API can execute large-scale **brute-force, password spraying, or credential stuffing** attacks without the device offering effective resistance, until obtaining valid administrator credentials. Successful exploitation grants full administrative access to the device, including configuration modification, access to stored credentials, persistence establishment, and use of the device as a pivot toward the internal network.

The risk is especially high when administration services (API, WinBox, WebFig) are exposed directly to the Internet or untrusted networks, which applies to a significant fraction of the more than 934,000 instances identified by ZoomEye.

Mitigation

As of the publication date of this bulletin, **no official patch is available** from MikroTik for CVE-2026-16347. The following mitigation measures must be applied immediately:

1. **Restrict access to the API and administration services**

Limit access to management services (API port 8728/8729, WinBox port 8291, WebFig/HTTPS, SSH, Telnet) exclusively to trusted administration IPs through firewall or ACLs in IP Services.

2. **Disable unnecessary administration services**

Disable Telnet, FTP, unencrypted HTTP WebFig, plain API (without SSL), proxy, SOCKS, UPnP, and remote DNS if they are not strictly required.

3. **Implement additional access controls**

Use IP whitelists on each enabled administration service in IP Services Allowed From.

4. **Enable two-factor authentication where possible**

Configure additional firewall rules that restrict API access only from management network segments.

5. **Check exposure in ZoomEye**

Identify whether the organization's devices appear exposed using the filter:

vul.cve="CVE-2026-16347" or the dork app="MikroTik RouterOS"

Search link: <https://www.zoomeye.hk/searchResult?q=vul.cve%3D%22CVE-2026-16347%22>

6. **Review authentication logs**

Search the router logs for massive failed authentication attempts or attempts from unknown IPs as an indicator of ongoing exploitation.

Solution

MikroTik has not published an official specific patch for CVE-2026-16347 as of the date of publication. It is recommended to:

Product	Patch status	Recommended action
MikroTik RouterOS – all versions	No patch available as of the date of publication	Apply the mitigations listed above and monitor the MikroTik security channel

Product	Patch status	Recommended action
MikroTik Cloud Hosted Router – all versions	No patch available as of the date of publication	Apply the mitigations listed above and monitor the MikroTik security channel

Monitor the official MikroTik security portal for the patch publication:

<https://mikrotik.com/supportsec>

Additional information:

- NVD – CVE-2026-16347
<https://nvd.nist.gov/vuln/detail/CVE-2026-16347>
- CISA – Advisory CVE-2026-16347
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Secarma – MikroTik routers vulnerable to rapid password brute forcing
<https://secarma.com/29-07-2026-mikrotik-authentication-vulnerability>
- Mallory.ai – Brute-forceable API Authentication in MikroTik RouterOS
<https://mallory.ai/vulnerabilities/CVE-2026-16347>
- ZoomEye – Search for exposed instances (CVE-2026-16347)
<https://www.zoomeye.hk/searchResult?q=vul.cve%3D%22CVE-2026-16347%22>
- MikroTik Forum – Technical discussion CVE-2026-16347
<https://forum.mikrotik.com/t/euvs-2026-50017-cve-2026-16347-ghsa-8v62-p5rj-72x6-which-routeros-version-does-fix-that/271934>
- MikroTik Security Portal
<https://mikrotik.com/supportsec>