

[HOME](#) / [SUPPORT](#) /

SECURITY

Responsible disclosure of discovered vulnerabilities

It is important for us at MikroTik that our customers can feel safe and secure when using our products. We therefore constantly strive to achieve the highest possible security and quality. Despite this, an issue could be discovered, that affects our device security. If you have found such a security flaw, we would like to hear more about it to be able to correct the problem as soon as possible.



We are thankful to you for taking the time to report to us weaknesses you discover, as long as you do so with adherence to the following responsible disclosure guidelines.

WHAT YOU CAN REPORT?



WHAT YOU SHOULD NOT REPORT?



IF YOU HAVE FOUND A VULNERABILITY, WE KINDLY ASK YOU TO:



WE PROMISE YOU THAT ...



SECURITY ANNOUNCEMENTS

[ALL](#) [2025](#) [2024](#) [2023](#) [2021](#) [2020](#) [2019](#) [2018](#)

CVE-2025-10948

Sep 25, 2025

A buffer overflow vulnerability has been discovered in MikroTik RouterOS 7, affecting the `parse_json_element` function within the `libjson.so` component. The vulnerability is triggered...

CVE-2025-6563

Jul 3, 2025

A cross-site scripting (XSS) vulnerability has been discovered in the hotspot functionality of MikroTik RouterOS, affecting versions below 7.19.2. An attacker can inject the...

CVE-2023-47310

Jun 30, 2025

A misconfiguration in the default settings of MikroTik RouterOS 7 allows incoming IPv6 UDP traceroute packets, which could permit unauthorized network reconnaissance from external...

CVE-2025-6443

Jun 25, 2025

An improper access control vulnerability has been identified in MikroTik RouterOS, related to the handling of VXLAN source IP addresses. This flaw allows remote attackers to bypass...

CVE-2024-54952

May 29, 2025

A memory corruption vulnerability has been discovered in the SMB service of MikroTik RouterOS. Remote, unauthenticated attackers can exploit this issue by sending specially...

CVE-2024-54772

Feb 18, 2025

Issue Summary

A vulnerability has been identified in the WinBox service, where a discrepancy in response...

CONTACT US ABOUT VULNERABILITIES

security@mikrotik.com[SUBSCRIBE TO OUR NEWSLETTER](#)

[illegible]



[Privacy Policy](#)