

Advisory on MikroTik RouterOS Vulnerability



A critical vulnerability in MikroTik RouterOS versions prior to 7.24 could allow remote code execution or denial of service. Institutions should prioritize updates to mitigate risks.

- The vulnerability allows remote code execution or denial of service.
- Affected versions are MikroTik RouterOS versions below 7.24.
- The issue is due to an integer underflow in the HTTP request handling.
- Exploitation can occur without authentication.
- MikroTik recommends updating to version 7.24 or later.

Overview

A critical vulnerability has been identified in MikroTik RouterOS versions prior to 7.24. This vulnerability could

enable attackers to execute arbitrary code remotely or cause a denial of service. The issue arises from an integer underflow in the HTTP request body handling, which is accessible before user authentication.

Impact

The exploitation of this vulnerability can have severe implications for organizations relying on affected MikroTik RouterOS versions. An unauthenticated attacker can leverage this flaw to gain root access or disrupt services, posing significant risks to operational integrity.

Recommended Actions

To mitigate the risks associated with this vulnerability, organizations are advised to take the following steps:

- Update MikroTik RouterOS to version 7.24 or later.
- Regularly review and monitor network configurations for unauthorized access attempts.
- Implement network segmentation to limit exposure of critical systems.
- Conduct vulnerability assessments to identify and remediate potential weaknesses.
- Stay informed about security advisories from MikroTik and relevant cybersecurity authorities.

What to do now

1. Update MikroTik RouterOS to version 7.24 or later.
2. Regularly review and monitor network configurations for unauthorized access attempts.
3. Implement network segmentation to limit exposure of critical systems.
4. Conduct vulnerability assessments to identify and remediate potential weaknesses.
5. Stay informed about security advisories from MikroTik and relevant cybersecurity authorities.