

MikroTik RouterOS Workflow Vulnerability Enables Unauthenticated Session Access



MikroTik RouterOS contains a workflow enforcement flaw allowing unauthenticated clients to open sessions and execute requests, which can be chained with another vulnerability for exploitation.

- CVE-2026-67279 affects MikroTik RouterOS with improper behavioral workflow enforcement
- Unauthenticated attackers can open session channels and send execution requests
- Vulnerability can be chained with CVE-2026-86060 for unauthenticated exploitation
- Vendor mitigations must be applied or product use discontinued if patches unavailable
- Organizations must evaluate internet exposure of affected assets and prioritize patching

Vulnerability Overview

MikroTik RouterOS has been found to contain an **improper enforcement of behavioral workflow** vulnerability tracked as CVE-2026-67279. The flaw permits unauthenticated clients to open session channels and send execution requests to affected devices. This represents a significant access control failure that bypasses normal authentication mechanisms.

The vulnerability becomes particularly concerning when combined with CVE-2026-86060, as the two can be chained together to achieve unauthenticated exploitation of RouterOS systems. This attack pattern increases the risk profile for organizations relying on MikroTik routing infrastructure.

Mitigation Requirements

Organizations operating MikroTik RouterOS devices must apply vendor-provided mitigations immediately. Where patches or mitigations are not available, institutions should discontinue use of the affected product until security updates become accessible. The vulnerability underscores the importance of maintaining current patch levels on network infrastructure.

Stakeholders are responsible for conducting thorough assessments of each asset's exposure to the internet. Devices directly accessible from untrusted networks face elevated risk and should be prioritized for remediation. Organizations should follow risk-based patching guidance and ensure that security updates are deployed systematically across their routing infrastructure.

Regulatory Considerations

For regulated institutions in the Kingdom, this vulnerability affects core network infrastructure that underpins critical operations. Proper documentation of assessment activities, remediation timelines, and compensating controls should be maintained to demonstrate compliance with applicable cybersecurity frameworks.

What to do now

1. Inventory all MikroTik RouterOS devices across your network infrastructure and determine their version status
2. Apply vendor-provided security updates and mitigations immediately to all affected RouterOS systems
3. Assess internet exposure of each MikroTik device and prioritize remediation for internet-facing assets
4. Implement network segmentation or access controls to limit exposure of RouterOS devices until patching is complete
5. Discontinue use of affected devices if vendor mitigations are unavailable or cannot be applied promptly
6. Document all assessment, remediation and compensating control activities for regulatory compliance purposes