



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



## Re: Two vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail.com>

Date: Tue, 4 May 2021 22:43:51 +0800

[Update 2021/05/04] Two CVEs have been assigned to these vulnerabilities.

CVE-2020-20221: Mikrotik RouterOs before 6.44.6 (long-term tree) suffers from an uncontrolled resource consumption vulnerability in the /nova/bin/cerm process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.

CVE-2020-20218: Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/traceroute process. An authenticated remote attacker can cause a Denial of Service due via the loop counter variable.

Q C <cq674350529 () gmail.com> 于2020年5月10日周日 上午10:41写道:

Advisory: two vulnerabilities found in MikroTik's RouterOS

### Details

Product: MikroTik's RouterOS  
Affected Versions: until stable 6.45.7 (first vulnerability), until stable 6.46.4 (second vulnerability)  
Fixed Versions: stable 6.46.x (first vulnerability), stable 6.46.5 (second vulnerability)  
Vendor URL: <https://mikrotik.com/>  
Vendor Status: fixed version released  
CVE: -  
Credit: Qian Chen (@cq674350529) of Qihoo 360 Nirvan Team

### Product Description

RouterOS is the operating system used on the MikroTik's devices, such as switch, router and access point.

### Description of vulnerabilities

These two vulnerabilities were tested only against the MikroTik RouterOS stable release tree when found. Maybe other release trees also suffer from these vulnerabilities.

1. The cerm process suffers from an uncontrolled resource consumption issue. By sending a crafted packet, an authenticated remote user can cause a high cpu load, which may make the device respond slowly or unable to respond.
2. The traceroute process suffers from a memory corruption issue. By sending a crafted packet, an authenticated remote user can crash the traceroute process due to invalid memory access.

### Solution

Upgrade to the corresponding latest RouterOS tree version.

### References

- [1] <https://mikrotik.com/download/changelogs/stable-release-tree>

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

### Current thread:

[Re: Two vulnerabilities found in MikroTik's RouterOS Q C \(May 04\)](#)

<Possible follow-ups>

[Re: Two vulnerabilities found in MikroTik's RouterOS Q C \(May 04\)](#)

[Re: Two vulnerabilities found in MikroTik's RouterOS Q C \(May 04\)](#)

[Re: Two vulnerabilities found in MikroTik's RouterOS Q C \(May 07\)](#)

Site Search



Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License

