



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 23:19:00 +0800

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

CVE-2020-20219: Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/igmp-proxy process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).

CVE-2020-20262: Mikrotik RouterOs before 6.47 (stable tree) suffers from an assertion failure vulnerability in the /ram/pkg/security/nova/bin/ipsec process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.

Q C <cq674350529 () gmail com> 于2020年8月13日周四 下午7:14写道:

Advisory: two vulnerabilities found in MikroTik's RouterOS

Details

Product: MikroTik's RouterOS
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

1. NULL pointer dereference

The igmpproxy process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the igmpproxy process due to NULL pointer dereference.

Against stable 6.46.5, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280: /ram/pkg/multicast/nova/bin/igmpproxy
2020.06.04-17:44:27.1280: --- signal=11
-----
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280: eip=0x08050a8d eflags=0x00010206
2020.06.04-17:44:27.1280: edi=0x7fa9331c esi=0x7fa932b8
ebp=0x7fa932a8 esp=0x7fa9326c
2020.06.04-17:44:27.1280: eax=0x080581bc ebx=0x00000000
ecx=0x0000000b edx=0x00000000
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280: maps:
2020.06.04-17:44:27.1280: 08048000-08053000 r-xp 00000000 00:13 16
/ram/pkg/multicast/nova/bin/igmpproxy
2020.06.04-17:44:27.1280: 7770b000-77740000 r-xp 00000000 00:0c 964
/lib/libuClibc-0.9.33.2.so
2020.06.04-17:44:27.1280: 77744000-7775e000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.04-17:44:27.1280: 7775f000-7776e000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.04-17:44:27.1280: 7776f000-77770000 r-xp 00000000 00:0c 950
/lib/libubox.so
2020.06.04-17:44:27.1280: 77778000-777c4000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.04-17:44:27.1280: 777ca000-777d1000 r-xp 00000000 00:0c 958
/lib/ld-uClibc-0.9.33.2.so
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280: stack: 0x7fa94000 - 0x7fa9326c
2020.06.04-17:44:27.1280: 01 00 00 00 e8 7f 05 08 10 00 00 98 32
a9 7f 11 00 00 00 78 57 05 08 14 33 a9 7f a8 32 a9 7f
2020.06.04-17:44:27.1280: 67 29 79 77 04 5d 05 08 6c 25 79 77 d8 32
a9 7f e0 57 05 08 b8 32 a9 7f 1c 33 a9 7f d8 32 a9 7f
2020.06.04-17:44:27.1280:
2020.06.04-17:44:27.1280: code: 0x8050a8d
2020.06.04-17:44:27.1280: 8b 03 ff 30 6a 01 56 e8 77 a8 ff ff 83 c4
0c 0f
```

This vulnerability was initially found in long-term 6.44.6, and was fixed in stable 6.47.

2. reachable assertion failure

The ipsec process suffers from an assertion failure vulnerability. There is a reachable assertion in the ipsec process. By sending a crafted packet, an authenticated remote user can crash the ipsec process due to assertion failure.

Against stable 6.46.5, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2020.06.04-18:25:16.0480:
2020.06.04-18:25:16.0480:
2020.06.04-18:25:16.0480: /ram/pkg/security/nova/bin/ipsec
2020.06.04-18:25:16.0480: --- signal=6
-----
2020.06.04-18:25:16.0480:
2020.06.04-18:25:16.0480: eip=0x7748155b eflags=0x00000246
2020.06.04-18:25:16.0480: edi=0x00000001 esi=0x77489200
ebp=0x7f8fa450 esp=0x7f8fa448
2020.06.04-18:25:16.0480: eax=0x00000000 ebx=0x00000291
ecx=0x00000291 edx=0x00000006
2020.06.04-18:25:16.0480:
2020.06.04-18:25:16.0480: maps:
2020.06.04-18:25:16.0480: 08048000-080b5000 r-xp 00000000 00:11 42
/ram/pkg/security/nova/bin/ipsec
2020.06.04-18:25:16.0480: 77453000-77488000 r-xp 00000000 00:0c 964
```

```
/lib/libuClibc-0.9.33.2.so
2020.06.04-18:25:16.04@0: 7748c000-774a6000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.04-18:25:16.04@0: 774a7000-774b6000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.04-18:25:16.04@0: 774b7000-774b9000 r-xp 00000000 00:0c 959
/lib/libdl-0.9.33.2.so
2020.06.04-18:25:16.04@0: 774bb000-774d0000 r-xp 00000000 00:1f 15
/cam/pkg/dhcp/lib/libudhcp.so
2020.06.04-18:25:16.04@0: 774d2000-774d8000 r-xp 00000000 00:0c 951
/lib/libradius.so
2020.06.04-18:25:16.04@0: 774d9000-77524000 r-xp 00000000 00:0c 956
/lib/libssl.so.1.0.0
2020.06.04-18:25:16.04@0: 77528000-77530000 r-xp 00000000 00:0c 950
/lib/libubox.so
2020.06.04-18:25:16.04@0: 77531000-7757d000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.04-18:25:16.04@0: 77580000-7759d000 r-xp 00000000 00:0c 947
/lib/libucrypto.so
2020.06.04-18:25:16.04@0: 7759e000-776fb000 r-xp 00000000 00:0c 954
/lib/libcrypto.so.1.0.0
2020.06.04-18:25:16.04@0: 7770e000-77715000 r-xp 00000000 00:0c 958
/lib/ld-uClibc-0.9.33.2.so
2020.06.04-18:25:16.04@0:
2020.06.04-18:25:16.04@0: stack: 0x7f8fb000 ~ 0x7f8fa448
2020.06.04-18:25:16.04@0: 00 90 48 77 00 90 48 77 88 a4 8f 7f 77 d0
47 77 06 00 00 00 00 92 48 77 20 00 00 00 00 00 00
2020.06.04-18:25:16.04@0: cc a4 8f 7f e8 a4 8f 7f 84 a4 8f 7f e4 da
57 77 01 00 00 00 e4 da 57 77 cc a4 8f 7f 01 00 00 00
2020.06.04-18:25:16.04@0:
2020.06.04-18:25:16.04@0: code: 0x7748155b
2020.06.04-18:25:16.04@0: 5b 3d 00 f0 ff ff 76 0e 8b 93 cc ff ff ff
f7 d8
```

This vulnerability was initially found in long-term 6.44.6, and was fixed in stable 6.47.

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

