



Site Search



[Full Disclosure](#) mailing list archives

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



List Archive Search



Four vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>

Date: Fri, 7 May 2021 16:56:02 +0800

Advisory: four vulnerabilities found in MikroTik's RouterOS

Details

=====

Product: MikroTik's RouterOS
Vendor URL: <https://mikrotik.com/>
Vendor Status: no fix yet
CVE: CVE-2020-20214, CVE-2020-20222, CVE-2020-20236, CVE-2020-20237
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 vulnerabilities were reported to the vendor almost one year ago. And the vendor confirmed these vulnerabilities. However, there is still no fix for them yet.
By the way, the three vulnerabilities in sniffer binary are different from each one.

1. CVE-2020-20214

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

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

```
# cat /rw/logs/backtrace.log
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940: /nova/bin/btest
2020.06.19-15:51:36.940: --- signal=6
-----
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940: eip=0x7772255b eflags=0x00000246
2020.06.19-15:51:36.940: edi=0x00fe0001 esi=0x7772a200 ebp=0x7fddf880
esp=0x7fddf878
2020.06.19-15:51:36.940: eax=0x00000000 ebx=0x0000010f ecx=0x0000010f
edx=0x00000006
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940: maps:
2020.06.19-15:51:36.940: 08048000-08057000 r-xp 00000000 00:0c 1006
/nova/bin/btest
2020.06.19-15:51:36.940: 776f4000-77729000 r-xp 00000000 00:0c 964
/lib/libuClibc-0.9.33.2.so
2020.06.19-15:51:36.940: 7772d000-77747000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.19-15:51:36.940: 77748000-77757000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.19-15:51:36.940: 77758000-77775000 r-xp 00000000 00:0c 947
/lib/libcrypto.so
2020.06.19-15:51:36.940: 77776000-777c2000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.19-15:51:36.940: 777c8000-777cf000 r-xp 00000000 00:0c 958
/lib/ld-uClibc-0.9.33.2.so
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940: stack: 0x7fdd0000 - 0x7fddf878
2020.06.19-15:51:36.940: 00 a0 72 77 00 a0 72 77 b8 f8 dc 7f 77 e0 71
77 06 00 00 00 a2 72 77 20 00 00 00 00 00 00
2020.06.19-15:51:36.940: 16 00 00 00 18 f9 dc 7f b4 f8 dc 7f e4 2a 7c
77 01 00 00 00 e4 2a 7c 77 16 00 00 00 01 00 fe 00
2020.06.19-15:51:36.940:
2020.06.19-15:51:36.940: code: 0x7772255b
2020.06.19-15:51:36.940: 5b 3d 00 f0 ff ff 76 0e 8b 93 cc ff ff ff f7
d8
```

This vulnerability was initially found in long-term 6.44.5, and it seems that the latest stable version 6.48.2 still suffers from this vulnerability.

2. CVE-2020-20222

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

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

```
# cat /rw/logs/backtrace.log
2020.06.19-16:36:18.330:
2020.06.19-16:36:18.330:
2020.06.19-16:36:18.330: /nova/bin/sniffer
2020.06.19-16:36:18.330: --- signal=11
-----
2020.06.19-16:36:18.330:
2020.06.19-16:36:18.330: eip=0x08050e33 eflags=0x00010206
2020.06.19-16:36:18.330: edi=0x08057a24 esi=0x7f85c094 ebp=0x7f85c0c8
esp=0x7f85c080
2020.06.19-16:36:18.330: eax=0x00000000 ebx=0x7f85c090 ecx=0x00ff0000
edx=0x08059678
2020.06.19-16:36:18.330:
2020.06.19-16:36:18.330: maps:
2020.06.19-16:36:18.330: 08048000-08056000 r-xp 00000000 00:0c 1034
/nova/bin/sniffer
2020.06.19-16:36:18.330: 776ce000-77703000 r-xp 00000000 00:0c 964
/lib/libuClibc-0.9.33.2.so
2020.06.19-16:36:18.330: 77707000-77721000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.19-16:36:18.330: 77722000-77731000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.19-16:36:18.330: 77732000-7773a000 r-xp 00000000 00:0c 950
/lib/libubox.so
2020.06.19-16:36:18.330: 7773b000-77787000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.19-16:36:18.330: 7778d000-77794000 r-xp 00000000 00:0c 958
/lib/ld-uClibc-0.9.33.2.so
```

```
2020.06.19-16:36:18.3380:
2020.06.19-16:36:18.3380: stack: 0x7f85d000 - 0x7f85c080
2020.06.19-16:36:18.3380: 2c 08 07 08 04 00 fe 08 fe 00 00 00 20 ad 05
08 00 0c 07 08 a0 0b 07 08 af 0b 07 08 04 7a 05 08
2020.06.19-16:36:18.3380: 08 00 00 00 24 7a 05 08 ff 00 00 00 00 00 00
00 08 c2 85 7f e4 7a 78 77 d8 c0 85 7f e4 7a 78 77
2020.06.19-16:36:18.3480:
2020.06.19-16:36:18.3480: code: 0x8050e33
2020.06.19-16:36:18.3480: 0b 48 0c 89 fa 89 d8 e8 7d f1 ff ff 50 50 53
56
```

This vulnerability was initially found in long-term 6.44.6, and it seems that the latest stable version 6.48.2 still suffers from this vulnerability.

3. CVE-2020-20236

The sniffer process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the sniffer process due to invalid memory access.

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

```
# cat /rw/logs/backtrace.log
2020.06.19-16:58:33.4280:
2020.06.19-16:58:33.4280:
2020.06.19-16:58:33.4280: /nova/bin/sniffer
2020.06.19-16:58:33.4280: --- signal=11
-----
2020.06.19-16:58:33.4280:
2020.06.19-16:58:33.4280: eip=0x08050dac eflags=0x00010202
2020.06.19-16:58:33.4280: edi=0x08057a24 esi=0x00000001 ebp=0x7f8df428
esp=0x7f8df3e0
2020.06.19-16:58:33.4280: eax=0x08073714 ebx=0x08073710 ecx=0x08073704
edx=0x08073714
2020.06.19-16:58:33.4280:
2020.06.19-16:58:33.4280: maps:
2020.06.19-16:58:33.4280: 08048000-08056000 r-xp 00000000 00:0c 1034
/nova/bin/sniffer
2020.06.19-16:58:33.4280: 77730000-77765000 r-xp 00000000 00:0c 964
/lib/libuClibc-0.9.33.2.so
2020.06.19-16:58:33.4280: 77769000-77783000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.19-16:58:33.4280: 77784000-77793000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.19-16:58:33.4280: 77794000-7779c000 r-xp 00000000 00:0c 950
/lib/libubox.so
2020.06.19-16:58:33.4280: 7779d000-777e9000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.19-16:58:33.4380: 777ef000-777f6000 r-xp 00000000 00:0c 958
/lib/libuClibc-0.9.33.2.so
2020.06.19-16:58:33.4380:
2020.06.19-16:58:33.4380: stack: 0x7f8e0000 - 0x7f8df3e0
2020.06.19-16:58:33.4380: 3c ab 05 08 04 00 fe 08 e0 0f 00 00 14 37 07
08 24 7a 05 08 00 00 00 18 f4 8d 7f 04 7a 05 08
2020.06.19-16:58:33.4380: 08 00 00 00 24 7a 05 08 04 00 00 00 00 00 00
00 70 4a 7a 77 e4 9a 7e 77 38 f4 8d 7f e4 9a 7e 77
2020.06.19-16:58:33.4380:
2020.06.19-16:58:33.4380: code: 0x8050dac
2020.06.19-16:58:33.4380: 8b 43 04 83 e0 fc 85 c0 74 1c 8b 4b 14 39 34
08
```

This vulnerability was initially found in long-term 6.46.3, and it seems that the latest version stable 6.48.2 still suffers from this vulnerability.

4. CVE-2020-20237

The sniffer process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the sniffer process due to invalid memory access.

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

```
# cat /rw/logs/backtrace.log
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880: /nova/bin/sniffer
2020.06.19-17:58:43.9880: --- signal=11
-----
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880: eip=0x77712055 eflags=0x00010202
2020.06.19-17:58:43.9880: edi=0x77720f34 esi=0x77721015 ebp=0x7ff96b38
esp=0x7ff96af8
2020.06.19-17:58:43.9880: eax=0x77721054 ebx=0x7771f000 ecx=0x77721034
edx=0x77721014
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880: maps:
2020.06.19-17:58:43.9880: 08048000-08056000 r-xp 00000000 00:0c 1034
/nova/bin/sniffer
2020.06.19-17:58:43.9880: 7776e9000-7777e000 r-xp 00000000 00:0c 964
/lib/libuClibc-0.9.33.2.so
2020.06.19-17:58:43.9880: 77722000-7773c000 r-xp 00000000 00:0c 960
/lib/libgcc_s.so.1
2020.06.19-17:58:43.9880: 7773d000-7774c000 r-xp 00000000 00:0c 944
/lib/libc++.so
2020.06.19-17:58:43.9880: 7774d000-77755000 r-xp 00000000 00:0c 950
/lib/libubox.so
2020.06.19-17:58:43.9880: 77756000-777a2000 r-xp 00000000 00:0c 946
/lib/libumsg.so
2020.06.19-17:58:43.9880: 777a8000-777af000 r-xp 00000000 00:0c 958
/lib/libuClibc-0.9.33.2.so
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880: stack: 0x7ff97000 - 0x7ff96af8
2020.06.19-17:58:43.9880: 00 f0 71 77 00 0f 72 77 30 00 00 00 00 00 00
00 38 b2 05 08 34 0f 72 77 04 00 00 00 00 0f 72 77
2020.06.19-17:58:43.9880: 20 00 00 00 1b 7b 71 77 e8 f1 71 77 98 00 00
00 01 00 00 00 ec c4 74 77 74 a1 05 08 f8 6b f9 7f
2020.06.19-17:58:43.9880:
2020.06.19-17:58:43.9880: code: 0x77712055
2020.06.19-17:58:43.9880: 89 14 10 eb bc 8b 93 a4 ff ff ff 8b 7d e0 8b
42
```

Interestingly, the same poc resulted in another different crash dump(SIGABRT) against stable 6.48.2.

```
# cat /rw/logs/backtrace.log
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580: /nova/bin/sniffer
2021.05.07-16:02:37.2580: --- signal=6
-----
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580: eip=0x776f255b eflags=0x00000246
2021.05.07-16:02:37.2580: edi=0x0805saca8 esi=0x776fa200 ebp=0x7f97def8
esp=0x7f97def0
2021.05.07-16:02:37.2580: eax=0x00000000 ebx=0x000000b6 ecx=0x000000b6
edx=0x00000006
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580: maps:
2021.05.07-16:02:37.2580: 08048000-08056000 r-xp 00000000 00:0c 1036
/nova/bin/sniffer
2021.05.07-16:02:37.2580: 776c4000-776f9000 r-xp 00000000 00:0c 966
/lib/libuClibc-0.9.33.2.so
2021.05.07-16:02:37.2580: 776fd000-77717000 r-xp 00000000 00:0c 962
/lib/libgcc_s.so.1
2021.05.07-16:02:37.2580: 77718000-77727000 r-xp 00000000 00:0c 945
/lib/libc++.so
2021.05.07-16:02:37.2580: 77728000-77730000 r-xp 00000000 00:0c 951
/lib/libubox.so
2021.05.07-16:02:37.2580: 77731000-7777d000 r-xp 00000000 00:0c 947
/lib/libumsg.so
2021.05.07-16:02:37.2580: 77783000-7778a000 r-xp 00000000 00:0c 960
/lib/libuClibc-0.9.33.2.so
```

```
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580: stack: 0x7f97f000 - 0x7f97def0
2021.05.07-16:02:37.2580: 00 a0 6f 77 00 a0 6f 77 30 df 97 7f 77 e0 6e
77 06 00 00 00 00 a2 6f 77 20 00 00 00 00 00 00
2021.05.07-16:02:37.2580: 26 2b 6f 77 00 a0 6f 77 28 df 97 7f 21 2c 6f
77 e8 a1 6f 77 00 a0 6f 77 00 bf 6f 77 a8 ac 05 08
2021.05.07-16:02:37.2580:
2021.05.07-16:02:37.2580: code: 0x776f255b
2021.05.07-16:02:37.2580: 5b 3d 00 f0 ff ff 76 0e 8b 93 cc ff ff ff f7
d8
```

This vulnerability was initially found in long-term 6.46.3, and it seems that the latest stable version 6.48.2 suffers from an assertion failure vulnerability when running the same poc.

Solution

No upgrade firmware available yet

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:

Four vulnerabilities found in MikroTik's RouterOS Q C (May 07)
<Possible follow-ups>
| [Four vulnerabilities found in MikroTik's RouterOS Q C \(May 11\)](#)

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

