

[Full Disclosure](#) mailing list archives[By Date](#) [By Thread](#)

Three vulnerabilities found in MikroTik's RouterOS

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

Date: Tue, 6 Jul 2021 19:26:29 +0800

Advisory: three 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) from Codesafe Team of Legendsec at Qi'anxin Group

Product Description

=====

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

Description of vulnerabilities

=====

1. reachable assertion failure

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

Against stable 6.47, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280: /ram/pkg/advanced-tools/nova/bin/netwatch
2020.06.29-14:27:25.5280: --- signal=6
-----
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280: eip=0x776b855b eflags=0x00000246
2020.06.29-14:27:25.5280: edi=0xffffffff esi=0x776c0200 ebp=0x7f6ea6a0
esp=0x7f6ea698
2020.06.29-14:27:25.5280: eax=0x00000000 ebx=0x000000b8 ecx=0x000000b8
edx=0x00000006
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280: maps:
2020.06.29-14:27:25.5280: 08048000-0804d000 r-xp 00000000 00:10 14
/ram/pkg/advanced-tools/nova/bin/netwatch
2020.06.29-14:27:25.5280: 7768a000-776bf000 r-xp 00000000 00:0c 966
/lib/libuClibc-0.9.33.2.so
2020.06.29-14:27:25.5280: 776c3000-776dd000 r-xp 00000000 00:0c 962
/lib/libgcc_s.so.1
2020.06.29-14:27:25.5280: 776de000-776ed000 r-xp 00000000 00:0c 945
/lib/libuc++.so
2020.06.29-14:27:25.5280: 776ee000-7773a000 r-xp 00000000 00:0c 947
/lib/libumsg.so
2020.06.29-14:27:25.5280: 77740000-77747000 r-xp 00000000 00:0c 960
/lib/ld-uClibc-0.9.33.2.so
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280: stack: 0x7f6eb000 ~ 0x7f6ea698
2020.06.29-14:27:25.5280: 00 00 6c 77 00 00 6c 77 d8 a6 ee 7f 77 40 6b
77 06 00 00 00 00 02 6c 77 20 00 00 00 00 00 00
2020.06.29-14:27:25.5280: bc b0 ee 7f 38 a7 ee 7f d4 a6 ee 7f f4 aa 73
77 b8 a6 ee 7f f4 aa 73 77 bc b0 ee 7f ff ff ff ff
2020.06.29-14:27:25.5280:
2020.06.29-14:27:25.5280: code: 0x776b855b
2020.06.29-14:27:25.5280: 5b 3d 00 f0 ff ff 76 0e 8b 93 cc ff ff ff f7
d8
```

This vulnerability was initially found in stable 6.46.2, and it seems that the latest stable version 6.48.3 still suffers from this vulnerability.

2. NULL pointer dereference

The tr069-client process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the tr069-client process due to NULL pointer dereference.

Against stable 6.47, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380: /ram/pkg/tr069-client/nova/bin/tr069-client
2020.06.10-17:04:17.6380: --- signal=11
-----
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380: eip=0x0805a185 eflags=0x00010206
2020.06.10-17:04:17.6380: edi=0x7ff74a04 esi=0x7ff74a04 ebp=0x7ff74988
esp=0x7ff7497c
2020.06.10-17:04:17.6380: eax=0x00000000 ebx=0x080a9290 ecx=0x776924ec
edx=0x7769187c
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380: maps:
2020.06.10-17:04:17.6380: 08048000-08096000 r-xp 00000000 00:10 13
/ram/pkg/tr069-client/nova/bin/tr069-client
2020.06.10-17:04:17.6380: 7762f000-77664000 r-xp 00000000 00:0c 966
/lib/libuClibc-0.9.33.2.so
2020.06.10-17:04:17.6380: 77668000-77682000 r-xp 00000000 00:0c 962
/lib/libgcc_s.so.1
2020.06.10-17:04:17.6380: 77683000-77692000 r-xp 00000000 00:0c 945
/lib/libuc++.so
2020.06.10-17:04:17.6380: 77693000-7769d000 r-xp 00000000 00:0c 963
/lib/libm-0.9.33.2.so
2020.06.10-17:04:17.6380: 7769f000-776bc000 r-xp 00000000 00:0c 948
/lib/libcrypto.so
2020.06.10-17:04:17.6380: 776bd000-776c0000 r-xp 00000000 00:0c 954
/lib/libxml.so
2020.06.10-17:04:17.6380: 776c1000-7770d000 r-xp 00000000 00:0c 947
/lib/libumsg.so
2020.06.10-17:04:17.6380: 77710000-7771b000 r-xp 00000000 00:0c 955
/lib/libuhttp.so
2020.06.10-17:04:17.6380: 7771c000-77724000 r-xp 00000000 00:0c 951
/lib/libubox.so
2020.06.10-17:04:17.6380: 77728000-7772f000 r-xp 00000000 00:0c 960
```

```
/lib/ld-uClibc-0.9.33.2.so
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380: stack: 0x7ff75000 - 0x7ff7497c
2020.06.10-17:04:17.6380: 10 a0 08 08 40 4b 72 77 90 92 0a 08 b8 49 f7
7f 7c fa 71 77 90 92 0a 08 04 4a f7 7f 05 00 00 00
2020.06.10-17:04:17.6380: 28 4a f7 7f b4 49 f7 7f 40 4b 72 77 88 5b 09
08 40 4b 72 77 80 4d f7 7f 04 4a f7 7f 28 4a f7 7f
2020.06.10-17:04:17.6380:
2020.06.10-17:04:17.6380: code: 0x805a185
2020.06.10-17:04:17.6380: ff 30 6a 01 56 e8 81 49 ff ff 83 c4 0c ff 73
24
```

This vulnerability was initially found in stable 6.47, and was fixed in stable 6.48.2.

3. NULL pointer dereference

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

Against stable 6.48.1, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2021.02.08-12:13:09.3380:
2021.02.08-12:13:09.3380: /nova/bin/ptp
2021.02.08-12:13:09.3380: --- signal=11
-----
2021.02.08-12:13:09.3380:
2021.02.08-12:13:09.3380: eip=0x08050abb eflags=0x00010202
2021.02.08-12:13:09.3380: edi=0x7fd5ee94 esi=0x0805be48 ebp=0x7fd5ee18
esp=0x7fd5ee18
2021.02.08-12:13:09.3380: eax=0x00000000 ebx=0x776f5b40 ecx=0x0805c6a8
edx=0x00000001
2021.02.08-12:13:09.3380:
2021.02.08-12:13:09.3380: maps:
2021.02.08-12:13:09.3380: 08048000-08058000 r-xp 00000000 00:0c 1067
/nova/bin/ptp
2021.02.08-12:13:09.3380: 7767d000-776b2000 r-xp 00000000 00:0c 966
/lib/libuClibc-0.9.33.2.so
2021.02.08-12:13:09.3380: 776b6000-776d0000 r-xp 00000000 00:0c 962
/lib/libgcc_s.so.1
2021.02.08-12:13:09.3380: 776d1000-776e0000 r-xp 00000000 00:0c 945
/lib/libc++.so
2021.02.08-12:13:09.3380: 776e1000-776eb000 r-xp 00000000 00:0c 963
/lib/libm-0.9.33.2.so
2021.02.08-12:13:09.3380: 776ed000-776f5000 r-xp 00000000 00:0c 951
/lib/libubox.so
2021.02.08-12:13:09.3380: 776f6000-77742000 r-xp 00000000 00:0c 947
/lib/libumsg.so
2021.02.08-12:13:09.3380: 77748000-7774f000 r-xp 00000000 00:0c 960
/lib/ld-uClibc-0.9.33.2.so
2021.02.08-12:13:09.3380:
2021.02.08-12:13:09.3380: stack: 0x7fd5f000 - 0x7fd5ee18
2021.02.08-12:13:09.3380: 48 ee d5 7f 7c 0a 6f 77 48 be 05 08 94 ee d5
7f 05 00 00 00 86 3c 71 77 f8 ef d5 7f 0c 00 fe 08
2021.02.08-12:13:09.3380: 58 ee d5 7f 40 5b 6f 77 a0 f1 d5 7f 94 ee d5
7f b8 ee d5 7f 16 41 6f 77 94 ee d5 7f a0 f1 d5 7f
2021.02.08-12:13:09.3380:
2021.02.08-12:13:09.3380: code: 0x8050abb
2021.02.08-12:13:09.3380: 8b 10 89 45 08 8b 42 18 5d ff e0 55 89 e5 31
c0
```

This vulnerability was initially found in stable 6.48.1, and was fixed in stable 6.48.2.

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:

Three vulnerabilities found in MikroTik's RouterOS *Q C (Jul 06)*

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

