Four vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>
Date: Tue, 11 May 2021 11:36:21 +0800

```
Advisory: four vulnerabilities found in MikroTik's RouterOS


Details
=======

Product: MikroTik's RouterOS
Vendor URL: https://mikrotik.com/
Vendor Status: only CVE-2020-20227 is fixed
CVE: CVE-2020-20220, CVE-2020-20227, CVE-2020-20245, CVE-2020-20246
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.

1. CVE-2020-20220
The bfd process suffers from a memory corruption vulnerability. By sending
a crafted packet, an authenticated remote user can crash the bfd process
due to invalid memory access.

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

    # cat /rw/logs/backtrace.log
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0: /ram/pckg/routing/nova/bin/bfd
    2020.06.19-18:36:13.88@0: --- signal=11
-------------------------------------------
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0: eip=0x0804b175 eflags=0x00010202
    2020.06.19-18:36:13.88@0: edi=0x08054a90 esi=0x08054298 ebp=0x7f9d3e88
esp=0x7f9d3e70
    2020.06.19-18:36:13.88@0: eax=0x08050634 ebx=0x77777af0 ecx=0x08051274
edx=0x00000001
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0: maps:
    2020.06.19-18:36:13.88@0: 08048000-08050000 r-xp 00000000 00:1b 16
    /ram/pckg/routing/nova/bin/bfd
    2020.06.19-18:36:13.88@0: 7759a000-7759c000 r-xp 00000000 00:0c 959
   /lib/libdl-0.9.33.2.so
    2020.06.19-18:36:13.88@0: 7759e000-775d3000 r-xp 00000000 00:0c 964
   /lib/libuClibc-0.9.33.2.so
    2020.06.19-18:36:13.88@0: 775d7000-775f1000 r-xp 00000000 00:0c 960
   /lib/libgcc_s.so.1
    2020.06.19-18:36:13.88@0: 775f2000-77601000 r-xp 00000000 00:0c 944
   /lib/libuc++.so
    2020.06.19-18:36:13.88@0: 77602000-7775f000 r-xp 00000000 00:0c 954
   /lib/libcrypto.so.1.0.0
    2020.06.19-18:36:13.88@0: 7776f000-77777000 r-xp 00000000 00:0c 950
   /lib/libubox.so
    2020.06.19-18:36:13.88@0: 77778000-777c4000 r-xp 00000000 00:0c 946
   /lib/libumsg.so
    2020.06.19-18:36:13.88@0: 777ca000-777d1000 r-xp 00000000 00:0c 958
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0: stack: 0x7f9d4000 - 0x7f9d3e70
    2020.06.19-18:36:13.88@0: 34 06 05 08 d0 e6 04 08 d8 3e 9d 7f 90 4a 05
08 98 42 05 08 d8 3e 9d 7f f8 3e 9d 7f 6d 39 77 77
    2020.06.19-18:36:13.88@0: 90 4a 05 08 28 40 9d 7f 05 00 00 00 00 43 05
08 00 00 00 00 28 90 7c 77 01 00 00 00 0c 00 00 00
    2020.06.19-18:36:13.88@0:
    2020.06.19-18:36:13.88@0: code: 0x804b175
    2020.06.19-18:36:13.88@0: ff 05 00 00 00 00 83 c4 10 c9 c3 55 89 e5 53
83

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

2. CVE-2020-20227
The diskd process suffers from a memory corruption vulnerability. By
sending a crafted packet, an authenticated remote user can crash the diskd
process due to invalid memory access.

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

    # cat /rw/logs/backtrace.log
    2020.06.05-15:00:38.33@0:
    2020.06.05-15:00:38.33@0:
    2020.06.05-15:00:38.33@0: /nova/bin/diskd
    2020.06.05-15:00:38.33@0: --- signal=11
-----------------------------------------------
    2020.06.05-15:00:38.33@0:
    2020.06.05-15:00:38.33@0: eip=0x7775a1e3 eflags=0x00010202
    2020.06.05-15:00:38.33@0: edi=0x7f9dd024 esi=0x0000000a ebp=0x7f9dceb8
esp=0x7f9dceac
    2020.06.05-15:00:38.33@0: eax=0x0000000a ebx=0x777624ec ecx=0x08054600
edx=0x08056e18
    2020.06.05-15:00:38.33@0:
    2020.06.05-15:00:38.33@0: maps:
    2020.06.05-15:00:38.33@0: 08048000-08052000 r-xp 00000000 00:0c 1049
    /nova/bin/diskd
    2020.06.05-15:00:38.33@0: 776ff000-77734000 r-xp 00000000 00:0c 966
   /lib/libuClibc-0.9.33.2.so
    2020.06.05-15:00:38.33@0: 77738000-77752000 r-xp 00000000 00:0c 962
   /lib/libgcc_s.so.1
    2020.06.05-15:00:38.33@0: 77753000-77762000 r-xp 00000000 00:0c 945
   /lib/libuc++.so
    2020.06.05-15:00:38.33@0: 77763000-7776b000 r-xp 00000000 00:0c 951
   /lib/libubox.so
    2020.06.05-15:00:38.33@0: 7776c000-777b8000 r-xp 00000000 00:0c 947
   /lib/libumsg.so
    2020.06.05-15:00:38.33@0: 777be000-777c5000 r-xp 00000000 00:0c 960
   /lib/ld-uClibc-0.9.33.2.so
```

```
    2020.06.05-15:00:38.33@0:
    2020.06.05-15:00:38.33@0: stack: 0x7f9de000 - 0x7f9dceac
    2020.06.05-15:00:38.33@0: f4 8a 7b 77 0a 00 00 00 f4 8a 7b 77 e8 ce 9d
7f 92 be 78 77 f8 45 05 08 0a 00 00 00 18 6e 05 08
    2020.06.05-15:00:38.33@0: 18 6e 05 08 e4 ce 9d 7f 24 d0 9d 7f 7c 18 76
77 24 d0 9d 7f 18 69 05 08 40 cf 9d 7f a8 cf 9d 7f
    2020.06.05-15:00:38.34@0:
    2020.06.05-15:00:38.34@0: code: 0x7775a1e3
    2020.06.05-15:00:38.34@0: 8b 00 8b 10 01 c2 83 c2 04 52 83 c0 04 50 ff
75
```

This vulnerability was initially found in stable 6.47, and it was fixed at least in stable 6.48.1.

3. CVE-2020-20245
The log process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the log process due to invalid memory access.

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

```
    # cat /rw/logs/backtrace.log
    2020.06.22-20:13:36.29@0:
    2020.06.22-20:13:36.29@0:
    2020.06.22-20:13:36.62@0: /nova/bin/log
    2020.06.22-20:13:36.62@0: --- signal=11
-------------------------------------------
    2020.06.22-20:13:36.62@0:
    2020.06.22-20:13:36.62@0: eip=0x77709d2e eflags=0x00010202
    2020.06.22-20:13:36.62@0: edi=0x0000004b esi=0x77718f00 ebp=0x7fec6858
esp=0x7fec6818
    2020.06.22-20:13:36.62@0: eax=0x00000031 ebx=0x77717000 ecx=0x777171e8
edx=0x00000006
    2020.06.22-20:13:36.62@0:
    2020.06.22-20:13:36.62@0: maps:
    2020.06.22-20:13:36.62@0: 08048000-08058000 r-xp 00000000 00:0c 1005
    /nova/bin/log
    2020.06.22-20:13:36.62@0: 776e1000-77716000 r-xp 00000000 00:0c 966
   /lib/libuClibc-0.9.33.2.so
    2020.06.22-20:13:36.62@0: 7771a000-77734000 r-xp 00000000 00:0c 962
   /lib/libgcc_s.so.1
    2020.06.22-20:13:36.62@0: 77735000-77744000 r-xp 00000000 00:0c 945
   /lib/libuc++.so
    2020.06.22-20:13:36.62@0: 77745000-77791000 r-xp 00000000 00:0c 947
   /lib/libumsg.so
    2020.06.22-20:13:36.62@0: 77797000-7779e000 r-xp 00000000 00:0c 960
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.22-20:13:36.62@0:
    2020.06.22-20:13:36.62@0: stack: 0x7fec7000 - 0x7fec6818
    2020.06.22-20:13:36.62@0: 48 68 ec 7f 7b ce 73 77 00 00 00 00 10 00 00
00 00 00 00 00 00 00 00 00 68 68 ec 7f 21 ac 70 77
    2020.06.22-20:13:36.62@0: 40 00 00 00 1b fb 70 77 e8 71 71 77 c0 28 06
08 88 68 ec 7f ec 44 74 77 e4 29 06 08 40 69 ec 7f
    2020.06.22-20:13:36.62@0:
    2020.06.22-20:13:36.62@0: code: 0x77709d2e
    2020.06.22-20:13:36.62@0: 8b 48 08 89 4c 96 04 e9 93 05 00 00 81 7d e0
ff
```

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

4. CVE-2020-20246
The mactel process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the mactel process due to NULL pointer dereference.

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

```
    # cat /rw/logs/backtrace.log
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0: /nova/bin/mactel
    2020.06.22-20:25:36.17@0: --- signal=11
-------------------------------------------
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0: eip=0x0804ddc7 eflags=0x00010202
    2020.06.22-20:25:36.17@0: edi=0x08055740 esi=0x7fe78144 ebp=0x7fe780c8
esp=0x7fe78090
    2020.06.22-20:25:36.17@0: eax=0x00000000 ebx=0x776b9b40 ecx=0x0000000b
edx=0xffffffff
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0: maps:
    2020.06.22-20:25:36.17@0: 08048000-08051000 r-xp 00000000 00:0c 1041
    /nova/bin/mactel
    2020.06.22-20:25:36.17@0: 7762c000-77661000 r-xp 00000000 00:0c 966
   /lib/libuClibc-0.9.33.2.so
    2020.06.22-20:25:36.17@0: 77665000-7767f000 r-xp 00000000 00:0c 962
   /lib/libgcc_s.so.1
    2020.06.22-20:25:36.17@0: 77680000-7768f000 r-xp 00000000 00:0c 945
   /lib/libuc++.so
    2020.06.22-20:25:36.17@0: 77690000-776ad000 r-xp 00000000 00:0c 948
   /lib/libucrypto.so
    2020.06.22-20:25:36.17@0: 776ae000-776af000 r-xp 00000000 00:0c 967
   /lib/libutil-0.9.33.2.so
    2020.06.22-20:25:36.17@0: 776b1000-776b9000 r-xp 00000000 00:0c 951
   /lib/libubox.so
    2020.06.22-20:25:36.17@0: 776ba000-77706000 r-xp 00000000 00:0c 947
   /lib/libumsg.so
    2020.06.22-20:25:36.17@0: 7770c000-77713000 r-xp 00000000 00:0c 960
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0: stack: 0x7fe79000 - 0x7fe78090
    2020.06.22-20:25:36.17@0: 44 81 e7 7f 01 00 00 00 ff ff ff ff 1f d0 04
08 58 57 05 08 28 b0 70 77 01 00 00 00 00 00 00 00
    2020.06.22-20:25:36.17@0: 1c 85 e7 7f 04 1d 05 08 02 db 70 77 40 9b 6b
77 40 57 05 08 44 81 e7 7f f8 80 e7 7f 7c 4a 6b 77
    2020.06.22-20:25:36.17@0:
    2020.06.22-20:25:36.17@0: code: 0x804ddc7
    2020.06.22-20:25:36.17@0: 8b 50 2f 89 55 da 66 8b 40 33 66 89 45 de 83
c4
```

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

Solution
========

As to CVE-2020-20227, upgrade to the corresponding latest RouterOS tree version. For others, no upgrade firmware available yet

References
==========

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

---

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)*