Mikrotik RouterOS 6.46.5 Memory Corruption / Assertion Failure

Authored by Qian Chen | Posted May 10, 2021

MikroTik RouterOS version 6.46.5 suffers from an assertion failure and multiple memory corruption vulnerabilities.

tags | advisory, vulnerability
advisories | CVE-2020-20214, CVE-2020-20222, CVE-2020-20236, CVE-2020-20237
SHA-256 | a64685676fca951c82952a48568cc23b987ea04f6128ac9fa93f1d10f7bfbe11 Download | Favorite | View

Related Files

Change Mirror Download

```
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
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480: /nova/bin/btest
    2020.06.19-15:51:36.9480: --- signal=6
-----------------------------------------------
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480: eip=0x7772255b eflags=0x00000246
    2020.06.19-15:51:36.9480: edi=0x00fe0001 esi=0x7772a200 ebp=0x7fdcf880
esp=0x7fdcf878
    2020.06.19-15:51:36.9480: eax=0x00000000 ebx=0x0000010f ecx=0x0000010f
edx=0x00000006
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480: maps:
    2020.06.19-15:51:36.9480: 08048000-08057000 r-xp 00000000 00:0c 1006
    /nova/bin/btest
    2020.06.19-15:51:36.9480: 776f4000-77729000 r-xp 00000000 00:0c 964
   /lib/libuClibc-0.9.33.2.so
    2020.06.19-15:51:36.9480: 7772d000-77747000 r-xp 00000000 00:0c 960
   /lib/libgcc_s.so.1
    2020.06.19-15:51:36.9480: 77748000-77757000 r-xp 00000000 00:0c 944
   /lib/libuc++.so
    2020.06.19-15:51:36.9480: 77758000-77775000 r-xp 00000000 00:0c 947
   /lib/libucrypto.so
    2020.06.19-15:51:36.9480: 77776000-777c2000 r-xp 00000000 00:0c 946
   /lib/libumsg.so
    2020.06.19-15:51:36.9480: 777c8000-777cf000 r-xp 00000000 00:0c 958
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480: stack: 0x7fdd0000 - 0x7fdcf878
    2020.06.19-15:51:36.9480: 00 a0 72 77 00 a0 72 77 b8 f8 dc 7f 77 e0 71
77 06 00 00 00 00 a2 72 77 20 00 00 00 00 00 00 00
    2020.06.19-15:51:36.9480: 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
    2020.06.19-15:51:36.9480:
    2020.06.19-15:51:36.9480: code: 0x7772255b
    2020.06.19-15:51:36.9480: 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
    2020.06.19-16:36:18.3380:
    2020.06.19-16:36:18.3380:
    2020.06.19-16:36:18.3380: /nova/bin/sniffer
    2020.06.19-16:36:18.3380: --- signal=11
-----------------------------------------------
    2020.06.19-16:36:18.3380:
    2020.06.19-16:36:18.3380: eip=0x08050e33 eflags=0x00010206
    2020.06.19-16:36:18.3380: edi=0x08057a24 esi=0x7f85c094 ebp=0x7f85c0c8
esp=0x7f85c080
    2020.06.19-16:36:18.3380: eax=0x00000000 ebx=0x7f85c090 ecx=0x00ff0000
edx=0x08059678
    2020.06.19-16:36:18.3380:
    2020.06.19-16:36:18.3380: maps:
    2020.06.19-16:36:18.3380: 08048000-08056000 r-xp 00000000 00:0c 1034
    /nova/bin/sniffer
    2020.06.19-16:36:18.3380: 776ce000-77703000 r-xp 00000000 00:0c 964
   /lib/libuClibc-0.9.33.2.so
    2020.06.19-16:36:18.3380: 77707000-77721000 r-xp 00000000 00:0c 960
   /lib/libgcc_s.so.1
    2020.06.19-16:36:18.3380: 77722000-77731000 r-xp 00000000 00:0c 944
   /lib/libuc++.so
    2020.06.19-16:36:18.3380: 77732000-7773a000 r-xp 00000000 00:0c 950
   /lib/libubox.so
    2020.06.19-16:36:18.3380: 7773b000-77787000 r-xp 00000000 00:0c 946
   /lib/libumsg.so
    2020.06.19-16:36:18.3380: 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
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- Older

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

```
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
    2020.06.19-16:58:33.42@0:
    2020.06.19-16:58:33.42@0:
    2020.06.19-16:58:33.42@0: /nova/bin/sniffer
    2020.06.19-16:58:33.42@0: --- signal=11
-----------------------------------------------
    2020.06.19-16:58:33.42@0:
    2020.06.19-16:58:33.42@0: eip=0x08050dac eflags=0x00010202
    2020.06.19-16:58:33.42@0: edi=0x08057a24 esi=0x00000001 ebp=0x7f8df428
esp=0x7f8df3e0
    2020.06.19-16:58:33.42@0: eax=0x08073714 ebx=0x08073710 ecx=0x08073704
edx=0x08073714
    2020.06.19-16:58:33.42@0:
    2020.06.19-16:58:33.42@0: maps:
    2020.06.19-16:58:33.42@0: 08048000-08056000 r-xp 00000000 00:0c 1034
    /nova/bin/sniffer
    2020.06.19-16:58:33.42@0: 77730000-77765000 r-xp 00000000 00:0c 964
   /lib/libuClibc-0.9.33.2.so
    2020.06.19-16:58:33.42@0: 77769000-77783000 r-xp 00000000 00:0c 960
   /lib/libgcc_s.so.1
    2020.06.19-16:58:33.42@0: 77784000-77793000 r-xp 00000000 00:0c 944
   /lib/libuc++.so
    2020.06.19-16:58:33.42@0: 77794000-7779c000 r-xp 00000000 00:0c 950
   /lib/libubox.so
    2020.06.19-16:58:33.42@0: 7779d000-777e9000 r-xp 00000000 00:0c 946
   /lib/libumsg.so
    2020.06.19-16:58:33.43@0: 777ef000-777f6000 r-xp 00000000 00:0c 958
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.19-16:58:33.43@0:
    2020.06.19-16:58:33.43@0: stack: 0x7f8e0000 - 0x7f8df3e0
    2020.06.19-16:58:33.43@0: 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
    2020.06.19-16:58:33.43@0: 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
    2020.06.19-16:58:33.43@0:
    2020.06.19-16:58:33.43@0: code: 0x8050dac
    2020.06.19-16:58:33.43@0: 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
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0: /nova/bin/sniffer
    2020.06.19-17:58:43.98@0: --- signal=11
-----------------------------------------------
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0: eip=0x77712055 eflags=0x00010202
    2020.06.19-17:58:43.98@0: edi=0x77720f34 esi=0x77721015 ebp=0x7ff96b38
esp=0x7ff96af8
    2020.06.19-17:58:43.98@0: eax=0x77721054 ebx=0x7771f000 ecx=0x77721034
edx=0x77721014
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0: maps:
    2020.06.19-17:58:43.98@0: 08048000-08056000 r-xp 00000000 00:0c 1034
    /nova/bin/sniffer
    2020.06.19-17:58:43.98@0: 776e9000-7771e000 r-xp 00000000 00:0c 964
   /lib/libuClibc-0.9.33.2.so
    2020.06.19-17:58:43.98@0: 77722000-7773c000 r-xp 00000000 00:0c 960
   /lib/libgcc_s.so.1
    2020.06.19-17:58:43.98@0: 7773d000-7774c000 r-xp 00000000 00:0c 944
   /lib/libuc++.so
    2020.06.19-17:58:43.98@0: 7774d000-77755000 r-xp 00000000 00:0c 950
   /lib/libubox.so
    2020.06.19-17:58:43.98@0: 77756000-777a2000 r-xp 00000000 00:0c 946
   /lib/libumsg.so
    2020.06.19-17:58:43.98@0: 777a8000-777af000 r-xp 00000000 00:0c 958
   /lib/ld-uClibc-0.9.33.2.so
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0: stack: 0x7ff97000 - 0x7ff96af8
    2020.06.19-17:58:43.98@0: 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
    2020.06.19-17:58:43.98@0: 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
    2020.06.19-17:58:43.98@0:
    2020.06.19-17:58:43.98@0: code: 0x77712055
    2020.06.19-17:58:43.98@0: 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
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0: /nova/bin/sniffer
    2021.05.07-16:02:37.25@0: --- signal=6
-----------------------------------------------
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0: eip=0x776f255b eflags=0x00000246
    2021.05.07-16:02:37.25@0: edi=0x0805aca8 esi=0x776fa200 ebp=0x7f97def8
esp=0x7f97def0
    2021.05.07-16:02:37.25@0: eax=0x00000000 ebx=0x000000b6 ecx=0x000000b6
edx=0x00000006
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0: maps:
    2021.05.07-16:02:37.25@0: 08048000-08056000 r-xp 00000000 00:0c 1036
    /nova/bin/sniffer
    2021.05.07-16:02:37.25@0: 776c4000-776f9000 r-xp 00000000 00:0c 966
   /lib/libuClibc-0.9.33.2.so
    2021.05.07-16:02:37.25@0: 776fd000-77717000 r-xp 00000000 00:0c 962
   /lib/libgcc_s.so.1
    2021.05.07-16:02:37.25@0: 77718000-77727000 r-xp 00000000 00:0c 945
   /lib/libuc++.so
    2021.05.07-16:02:37.25@0: 77728000-77730000 r-xp 00000000 00:0c 951
   /lib/libubox.so
    2021.05.07-16:02:37.25@0: 77731000-7777d000 r-xp 00000000 00:0c 947
   /lib/libumsg.so
    2021.05.07-16:02:37.25@0: 77783000-7778a000 r-xp 00000000 00:0c 960
   /lib/ld-uClibc-0.9.33.2.so
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0: stack: 0x7f97f000 - 0x7f97def0
    2021.05.07-16:02:37.25@0: 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 00
    2021.05.07-16:02:37.25@0: 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
    2021.05.07-16:02:37.25@0:
    2021.05.07-16:02:37.25@0: code: 0x776f255b
    2021.05.07-16:02:37.25@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 6.46.3, 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
```

packet storm

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed