Re: Four vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>
Date: Wed, 5 May 2021 14:39:14 +0800

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

 CVE-2020-20254: Mikrotik RouterOs before 6.47 (stable tree) suffers from a
memory corruption vulnerability in the /nova/bin/lcdstat process. An
authenticated remote attacker can cause a Denial of Service (NULL pointer
dereference).

CVE-2020-20253: Mikrotik RouterOs before 6.47 (stable tree) in the
/nova/bin/lcdstat process. An authenticated remote attacker can cause a
Denial of Service due to a divide by zero error.

Q C <cq674350529 () gmail com> 于2020年7月7日周二 下午10:05写道:

> Advisory: four vulnerabilities found in MikroTik's RouterOS
>
>
> Details
> =======
>
> Product: MikroTik's RouterOS
> Affected Versions: through stable 6.47
> Fixed Versions: stable 6.47
> 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
> ===========================
>
> These four vulnerabilities were tested only against the MikroTik RouterOS
> stable release tree when found.
> Maybe other release trees also suffer from these vulnerabilities.
>
> PS: The following three memory corruption vulnerabilities are different.
>
> 1. NULL pointer dereference vulnerability
> The lcdstat process suffers from a memory corruption vulnerability. By
> sending a crafted packet,
> an authenticated remote user can crash the lcdstat process due to NULL
> pointer dereference.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0: /nova/bin/lcdstat
>   2020.06.04-15:32:04.67@0: --- signal=11
> --
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0: eip=0x0805a26e eflags=0x00010202
>   2020.06.04-15:32:04.67@0: edi=0x00000000 esi=0x7fbeaedc
> ebp=0x7fbeae18 esp=0x7fbeadf4
>   2020.06.04-15:32:04.67@0: eax=0x00000000 ebx=0x7fbeb848
> ecx=0x0807f14c edx=0x00000001
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0: maps:
>   2020.06.04-15:32:04.67@0: 08048000-0807e000 r-xp 00000000 00:0c 1054
>   /nova/bin/lcdstat
>   2020.06.04-15:32:04.67@0: 776fd000-77732000 r-xp 00000000 00:0c 964
>   /lib/libuClibc-0.9.33.2.so
>   2020.06.04-15:32:04.67@0: 77736000-77750000 r-xp 00000000 00:0c 960
>   /lib/libgcc_s.so.1
>   2020.06.04-15:32:04.67@0: 77751000-77760000 r-xp 00000000 00:0c 944
>   /lib/libuc++.so
>   2020.06.04-15:32:04.67@0: 77761000-77769000 r-xp 00000000 00:0c 950
>   /lib/libubox.so
>   2020.06.04-15:32:04.67@0: 7776a000-777b6000 r-xp 00000000 00:0c 946
>   /lib/libumsg.so
>   2020.06.04-15:32:04.67@0: 777bc000-777c3000 r-xp 00000000 00:0c 958
>   /lib/ld-uClibc-0.9.33.2.so
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0: stack: 0x7fbeb000 - 0x7fbeadf4
>   2020.06.04-15:32:04.67@0: 48 b8 be 7f 18 ae be 7f 95 ab 05 08 a0 e5
> 07 08 00 00 00 00 4c f1 07 08 48 b8 be 7f dc ae be 7f
>   2020.06.04-15:32:04.67@0: 00 00 00 00 58 ae be 7f 00 ad 05 08 48 b8
> be 7f 00 00 00 00 00 00 00 00 ec 04 76 77 d8 af be 7f
>   2020.06.04-15:32:04.67@0:
>   2020.06.04-15:32:04.67@0: code: 0x805a26e
>   2020.06.04-15:32:04.67@0: 8b 70 fc ff 73 78 e8 1f c0 ff ff 8b 46 10
> 83 c4
>
> 2. NULL pointer dereference vulnerability
> The lcdstat process suffers from a memory corruption vulnerability. By
> sending a crafted packet,
> an authenticated remote user can crash the lcdstat process due to NULL
> pointer dereference.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.04-15:48:13.77@0:
>   2020.06.04-15:48:13.77@0:
>   2020.06.04-15:48:13.77@0: /nova/bin/lcdstat
>   2020.06.04-15:48:13.77@0: --- signal=11
> --
>   2020.06.04-15:48:13.77@0:
>   2020.06.04-15:48:13.77@0: eip=0x080562c6 eflags=0x00010246
>   2020.06.04-15:48:13.77@0: edi=0xff000000 esi=0x00ff0000
> ebp=0x7fd8cb48 esp=0x7fd8cb2c
>   2020.06.04-15:48:13.77@0: eax=0x00000000 ebx=0x00000000

```
ecx=0x00000000 edx=0x00000000
    2020.06.04-15:48:13.77@0:
    2020.06.04-15:48:13.77@0: maps:
    2020.06.04-15:48:13.77@0: 08048000-0807e000 r-xp 00000000 00:0c 1054
      /nova/bin/lcdstat
    2020.06.04-15:48:13.77@0: 776be000-776f3000 r-xp 00000000 00:0c 964
     /lib/libuClibc-0.9.33.2.so
    2020.06.04-15:48:13.77@0: 776f7000-77711000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-15:48:13.77@0: 77712000-77721000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-15:48:13.77@0: 77722000-7772a000 r-xp 00000000 00:0c 950
     /lib/libubox.so
    2020.06.04-15:48:13.77@0: 7772b000-77777000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-15:48:13.77@0: 7777d000-77784000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-15:48:13.77@0:
    2020.06.04-15:48:13.77@0: stack: 0x7fd8d000 - 0x7fd8cb2c
    2020.06.04-15:48:13.77@0: 00 00 00 00 00 00 00 01 80 c1 77 77 01 00
00 00 38 d4 d8 7f 50 5f 08 08 a8 5c 08 08 78 cb d8 7f
    2020.06.04-15:48:13.77@0: 79 a2 05 08 78 36 08 08 00 00 00 00 00 de
77 77 8f cf d8 7f ff ff ff ff a8 5d 08 08 00 36 08 08
    2020.06.04-15:48:13.77@0:
    2020.06.04-15:48:13.77@0: code: 0x80562c6
    2020.06.04-15:48:13.77@0: 88 1c 02 89 f3 88 5c 02 01 89 fb 88 5c 02
02 05
```

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

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

```
    # cat /rw/logs/backtrace.log
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0: /nova/bin/lcdstat
    2020.06.04-15:58:23.76@0: --- signal=11
-----------------------------------------------
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0: eip=0x0805b566 eflags=0x00010202
    2020.06.04-15:58:23.76@0: edi=0x08085e70 esi=0x08085bf8
ebp=0x7fc0fca8 esp=0x7fc0fc70
    2020.06.04-15:58:23.76@0: eax=0x00000000 ebx=0x7fc106c8
ecx=0x0807f14c edx=0x00000001
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0: maps:
    2020.06.04-15:58:23.76@0: 08048000-0807e000 r-xp 00000000 00:0c 1054
      /nova/bin/lcdstat
    2020.06.04-15:58:23.76@0: 77680000-776b5000 r-xp 00000000 00:0c 964
     /lib/libuClibc-0.9.33.2.so
    2020.06.04-15:58:23.76@0: 776b9000-776d3000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-15:58:23.76@0: 776d4000-776e3000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-15:58:23.76@0: 776e4000-776ec000 r-xp 00000000 00:0c 950
     /lib/libubox.so
    2020.06.04-15:58:23.76@0: 776ed000-77739000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-15:58:23.76@0: 7773f000-77746000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0: stack: 0x7fc10000 - 0x7fc0fc70
    2020.06.04-15:58:23.76@0: e4 9a 73 77 58 fe c0 7f a8 fc c0 7f 00 00
00 00 58 fe c0 7f 73 00 00 00 9c fc c0 7f 22 ac 70 77
    2020.06.04-15:58:23.76@0: 58 fe c0 7f 72 00 00 08 b8 fc c0 7f 5c fd
c0 7f 70 5e 08 08 c8 06 c1 7f c8 fc c0 7f ab b8 05 08
    2020.06.04-15:58:23.76@0:
    2020.06.04-15:58:23.76@0: code: 0x805b566
    2020.06.04-15:58:23.76@0: 80 78 08 00 75 0c 52 52 50 53 e8 91 e7 ff
ff 83
```

4. division-by-zero vulnerability
The lcdstat process suffers from a division-by-zero vulnerability. By
sending a crafted packet,
an authenticated remote user can crash the lcdstat process due to
arithmetic exception.

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

```
    # cat /rw/logs/backtrace.log
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0: /nova/bin/lcdstat
    2020.06.04-16:17:48.62@0: --- signal=8
-----------------------------------------------
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0: eip=0x08058539 eflags=0x00010297
    2020.06.04-16:17:48.62@0: edi=0x0808b0c8 esi=0x00000000
ebp=0x7fffef88 esp=0x7fffef50
    2020.06.04-16:17:48.62@0: eax=0x00000008 ebx=0x7ffff030
ecx=0x00000000 edx=0x00000000
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0: maps:
    2020.06.04-16:17:48.62@0: 08048000-0807e000 r-xp 00000000 00:0c 1054
      /nova/bin/lcdstat
    2020.06.04-16:17:48.62@0: 77f38000-77f6d000 r-xp 00000000 00:0c 964
     /lib/libuClibc-0.9.33.2.so
    2020.06.04-16:17:48.62@0: 77f71000-77f8b000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-16:17:48.62@0: 77f8c000-77f9b000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-16:17:48.62@0: 77f9c000-77fa4000 r-xp 00000000 00:0c 950
     /lib/libubox.so
    2020.06.04-16:17:48.62@0: 77fa5000-77ff1000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-16:17:48.62@0: 77ff7000-77ffe000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0: stack: 0x80000000 - 0x7fffef50
    2020.06.04-16:17:48.62@0: 64 ef ff 7f ec b4 f9 77 84 b2 f9 77 ec b4
f9 77 a4 ef ff 7f 01 00 00 00 00 50 00 00 00 00 00 00
    2020.06.04-16:17:48.62@0: a4 ef ff 7f 74 5e 08 08 14 00 00 00 30 f0
ff 7f a4 ef ff 7f 28 f0 ff 7f e8 ef ff 7f cc 8e 05 08
    2020.06.04-16:17:48.62@0:
    2020.06.04-16:17:48.62@0: code: 0x8058539
    2020.06.04-16:17:48.62@0: f7 f9 89 45 e0 b8 01 00 00 00 d3 e0 48 31
ff 8b
```

Solution
========

Upgrade to the corresponding latest RouterOS tree version.

References
==========

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

Current thread:

Re: Four vulnerabilities found in MikroTik's RouterOS *Q C (May 07)*