Re: Two vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>
Date: Wed, 5 May 2021 14:14:26 +0800

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

CVE-2020-20267: Mikrotik RouterOs before 6.47 (stable tree) suffers from a
memory corruption vulnerability in the /nova/bin/resolver process. An
authenticated remote attacker can cause a Denial of Service due to invalid
memory access.

CVE-2020-20225: Mikrotik RouterOs before 6.47 (stable tree) suffers from an
assertion failure vulnerability in the /nova/bin/user process. An
authenticated remote attacker can cause a Denial of Service due to an
assertion failure via a crafted packet.

Q C <cq674350529 () gmail com> 于2020年9月9日周三 下午9:02写道:

> Advisory: two 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) 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
> ===========================
>
> 1. memory corruption
> The resolver process suffers from a memory corruption vulnerability. By
> sending a crafted packet, an authenticated remote user can crash the
> resolver process due to invalid memory access.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.18-14:38:03.27@0:
>   2020.06.18-14:38:03.27@0:
>   2020.06.18-14:38:03.28@0: /nova/bin/resolver
>   2020.06.18-14:38:03.28@0: --- signal=11
> ---
>   2020.06.18-14:38:03.28@0:
>   2020.06.18-14:38:03.28@0: eip=0x080508f6 eflags=0x00010206
>   2020.06.18-14:38:03.28@0: edi=0x08060620 esi=0x08062018
> ebp=0x7fe5fd08 esp=0x7fe5fcc0
>   2020.06.18-14:38:03.28@0: eax=0x0000000c ebx=0x08061c98
> ecx=0x77676f00 edx=0x00000005
>   2020.06.18-14:38:03.28@0:
>   2020.06.18-14:38:03.28@0: maps:
>   2020.06.18-14:38:03.28@0: 08048000-0805c000 r-xp 00000000 00:0c 995
>   /nova/bin/resolver
>   2020.06.18-14:38:03.28@0: 7763f000-77674000 r-xp 00000000 00:0c 964
>   /lib/libuClibc-0.9.33.2.so
>   2020.06.18-14:38:03.28@0: 77678000-77692000 r-xp 00000000 00:0c 960
>   /lib/libgcc_s.so.1
>   2020.06.18-14:38:03.28@0: 77693000-776a2000 r-xp 00000000 00:0c 944
>   /lib/libuc++.so
>   2020.06.18-14:38:03.28@0: 776a3000-776ab000 r-xp 00000000 00:0c 950
>   /lib/libubox.so
>   2020.06.18-14:38:03.28@0: 776ac000-776f8000 r-xp 00000000 00:0c 946
>   /lib/libumsg.so
>   2020.06.18-14:38:03.28@0: 776fe000-77705000 r-xp 00000000 00:0c 958
>   /lib/ld-uClibc-0.9.33.2.so
>   2020.06.18-14:38:03.28@0:
>   2020.06.18-14:38:03.28@0: stack: 0x7fe60000 - 0x7fe5fcc0
>   2020.06.18-14:38:03.28@0: 03 00 00 00 e4 8a 6f 77 38 fd e5 7f e4 fc
> e5 7f c0 dc 05 08 5c 03 e6 7f 08 fd e5 7f 1f e7 04 08
>   2020.06.18-14:38:03.28@0: 58 21 06 08 48 06 06 08 f8 1f 06 08 c0 0c
> 00 00 1c fd e5 7f 28 c7 05 08 02 fb 6f 77 98 1c 06 08
>   2020.06.18-14:38:03.28@0:
>   2020.06.18-14:38:03.28@0: code: 0x80508f6
>   2020.06.18-14:38:03.28@0: 88 10 8b 43 14 40 89 43 14 8b 55 dc 8d 72
> 04 8b
>
> This vulnerability was initially found in long-term 6.44.6, and was fixed
> in stable 6.47.
>
> 2. reachable assertion failure
> The user process suffers from an assertion failure vulnerability. There is
> a reachable assertion in the user process. By sending a crafted packet, an
> authenticated remote user can crash the user process due to assertion
> failure.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.04-17:56:52.31@0:
>   2020.06.04-17:56:52.31@0:
>   2020.06.04-17:56:52.31@0: /nova/bin/user
>   2020.06.04-17:56:52.31@0: --- signal=6
> ---
>   2020.06.04-17:56:52.31@0:
>   2020.06.04-17:56:52.31@0: eip=0x7765a55b eflags=0x00000246
>   2020.06.04-17:56:52.31@0: edi=0x00fe0001 esi=0x77662200
> ebp=0x7fee3790 esp=0x7fee3788
>   2020.06.04-17:56:52.31@0: eax=0x00000000 ebx=0x000000b4
> ecx=0x000000b4 edx=0x00000006
>   2020.06.04-17:56:52.31@0:
>   2020.06.04-17:56:52.31@0: maps:
>   2020.06.04-17:56:52.31@0: 08048000-08059000 r-xp 00000000 00:0c 1002
>   /nova/bin/user
>   2020.06.04-17:56:52.31@0: 7762c000-77661000 r-xp 00000000 00:0c 964
>   /lib/libuClibc-0.9.33.2.so

```
    2020.06.04-17:56:52.31@0: 77665000-7767f000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-17:56:52.31@0: 77680000-7768f000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-17:56:52.31@0: 77690000-776ad000 r-xp 00000000 00:0c 947
     /lib/libucrypto.so
    2020.06.04-17:56:52.31@0: 776ae000-776b4000 r-xp 00000000 00:0c 951
     /lib/liburadius.so
    2020.06.04-17:56:52.31@0: 776b5000-776bd000 r-xp 00000000 00:0c 950
     /lib/libubox.so
    2020.06.04-17:56:52.31@0: 776be000-776c1000 r-xp 00000000 00:0c 948
     /lib/libuxml++.so
    2020.06.04-17:56:52.31@0: 776c2000-7770e000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-17:56:52.31@0: 77714000-7771b000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-17:56:52.31@0:
    2020.06.04-17:56:52.31@0: stack: 0x7fee4000 - 0x7fee3788
    2020.06.04-17:56:52.31@0: 00 20 66 77 00 20 66 77 c8 37 ee 7f 77 60
65 77 06 00 00 00 00 22 66 77 20 00 00 00 00 00 00 00
    2020.06.04-17:56:52.31@0: 15 00 00 00 28 38 ee 7f c4 37 ee 7f e4 ea
70 77 01 00 00 00 e4 ea 70 77 15 00 00 00 01 00 fe 00
    2020.06.04-17:56:52.31@0:
    2020.06.04-17:56:52.31@0: code: 0x7765a55b
    2020.06.04-17:56:52.31@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 6.44.6, and was fixed
in stable 6.47.


Solution
========

Upgrade to the corresponding latest RouterOS tree version.


References
==========

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