Re: Three vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>
Date: Tue, 4 May 2021 23:56:26 +0800

[Update 2021/05/04] Three CVEs have been assigned to these vulnerabilities.

CVE-2020-20266: Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/dot1x process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).

CVE-2020-20264: Mikrotik RouterOs before 6.47 (stable tree) in the /ram/pckg/advanced-tools/nova/bin/netwatch process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.

CVE-2020-20265: Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /ram/pckg/wireless/nova/bin/wireless process. An authenticated remote attacker can cause a Denial of Service due via a crafted packet.

Q C <cq674350529 () gmail com> 于2020年8月27日周四 下午7:16写道:

> 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) 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. NULL pointer dereference
> The dot1x process suffers from a memory corruption vulnerability. By
> sending a crafted packet, an authenticated remote user can crash the dot1x
> process due to NULL pointer dereference.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.04-14:51:29.47@0:
>   2020.06.04-14:51:29.47@0:
>   2020.06.04-14:51:29.81@0: /nova/bin/dot1x
>   2020.06.04-14:51:29.81@0: --- signal=11
> ---
>   2020.06.04-14:51:29.81@0:
>   2020.06.04-14:51:29.81@0: eip=0x776a51e5 eflags=0x00010202
>   2020.06.04-14:51:29.81@0: edi=0x7fc51064 esi=0x08062ed0
> ebp=0x7fc50f78 esp=0x7fc50f6c
>   2020.06.04-14:51:29.81@0: eax=0x00000000 ebx=0x776ad4ec
> ecx=0x00000000 edx=0x08062e28
>   2020.06.04-14:51:29.81@0:
>   2020.06.04-14:51:29.81@0: maps:
>   2020.06.04-14:51:29.81@0: 08048000-0805f000 r-xp 00000000 00:0c 1064
>   /nova/bin/dot1x
>   2020.06.04-14:51:29.81@0: 7764a000-7767f000 r-xp 00000000 00:0c 964
>   /lib/libuClibc-0.9.33.2.so
>   2020.06.04-14:51:29.81@0: 77683000-7769d000 r-xp 00000000 00:0c 960
>   /lib/libgcc_s.so.1
>   2020.06.04-14:51:29.81@0: 7769e000-776ad000 r-xp 00000000 00:0c 944
>   /lib/libuc++.so
>   2020.06.04-14:51:29.81@0: 776ae000-776b4000 r-xp 00000000 00:0c 951
>   /lib/liburadius.so
>   2020.06.04-14:51:29.81@0: 776b5000-776bd000 r-xp 00000000 00:0c 950
>   /lib/libubox.so
>   2020.06.04-14:51:29.81@0: 776be000-776db000 r-xp 00000000 00:0c 947
>   /lib/libucrypto.so
>   2020.06.04-14:51:29.81@0: 776dc000-77728000 r-xp 00000000 00:0c 946
>   /lib/libumsg.so
>   2020.06.04-14:51:29.81@0: 7772e000-77735000 r-xp 00000000 00:0c 958
>   /lib/ld-uClibc-0.9.33.2.so
>   2020.06.04-14:51:29.81@0:
>   2020.06.04-14:51:29.81@0: stack: 0x7fc52000 - 0x7fc50f6c
>   2020.06.04-14:51:29.81@0: 00 00 00 00 90 27 06 08 e4 8a 72 77 a8 0f
> c5 7f 2e be 6f 77 90 27 06 08 d0 2e 06 08 28 2e 06 08
>   2020.06.04-14:51:29.81@0: 28 2e 06 08 a4 0f c5 7f f0 da 6b 77 05 00
> 00 00 f0 da 6b 77 e0 2d 06 08 64 10 c5 7f e8 0f c5 7f
>   2020.06.04-14:51:29.81@0:
>   2020.06.04-14:51:29.81@0: code: 0x776a51e5
>   2020.06.04-14:51:29.81@0: 8b 10 01 c2 83 c2 04 52 83 c0 04 50 ff 75
> 08 e8
>
> This vulnerability was initially found in stable 6.46.3, and was fixed in
> stable 6.47.
>
> 2. division by zero
> The netwatch process suffers from a division-by-zero vulnerability. By
> sending a crafted packet, an authenticated remote user can crash the
> netwatch process due to arithmetic exception.
>
> Against stable 6.46.5, the poc resulted in the following crash dump.
>
>   # cat /rw/logs/backtrace.log
>   2020.06.04-16:25:57.65@0:
>   2020.06.04-16:25:57.65@0:
>   2020.06.04-16:25:57.65@0: /ram/pckg/advanced-tools/nova/bin/netwatch
>   2020.06.04-16:25:57.65@0: --- signal=8
> ---
>   2020.06.04-16:25:57.65@0:
>   2020.06.04-16:25:57.65@0: eip=0x0804c6d7 eflags=0x00010246

```
    2020.06.04-16:25:57.65@0: edi=0x5ed9208c esi=0x00000000
ebp=0x7ffff3f8 esp=0x7ffff3b0
    2020.06.04-16:25:57.65@0: eax=0x00000000 ebx=0x08051020
ecx=0x00000000 edx=0x00000000
    2020.06.04-16:25:57.65@0:
    2020.06.04-16:25:57.65@0: maps:
    2020.06.04-16:25:57.65@0: 08048000-0804d000 r-xp 00000000 00:1a 14
      /ram/pckg/advanced-tools/nova/bin/netwatch
    2020.06.04-16:25:57.65@0: 77f41000-77f76000 r-xp 00000000 00:0c 964
     /lib/libuClibc-0.9.33.2.so
    2020.06.04-16:25:57.65@0: 77f7a000-77f94000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-16:25:57.65@0: 77f95000-77fa4000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-16:25:57.65@0: 77fa5000-77ff1000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-16:25:57.65@0: 77ff7000-77ffe000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-16:25:57.65@0:
    2020.06.04-16:25:57.65@0: stack: 0x80000000 - 0x7ffff3b0
    2020.06.04-16:25:57.65@0: d8 f4 ff 7f 80 f6 ff 7f 06 00 00 00 d0 f3
ff 7f 84 e5 04 08 0b 00 ff 08 e8 f3 ff 7f 06 00 00 00
    2020.06.04-16:25:57.65@0: 20 10 05 08 e4 1a ff 77 f8 f3 ff 7f 22 2c
fc 77 d8 f4 ff 7f 0b 00 ff 08 08 f4 ff 7f e4 1a ff 77
    2020.06.04-16:25:57.65@0:
    2020.06.04-16:25:57.65@0: code: 0x804c6d7
    2020.06.04-16:25:57.65@0: f7 f6 8b 53 30 39 c2 73 6e 42 89 53 30 83
ec 0c

This vulnerability was initially found in stable 6.46.2, and was fixed in
stable 6.47.

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

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

    # cat /rw/logs/backtrace.log
    2020.06.04-18:12:52.69@0:
    2020.06.04-18:12:52.69@0: /ram/pckg/wireless/nova/bin/wireless
    2020.06.04-18:12:52.69@0: --- signal=11
-----------------------------------------------
    2020.06.04-18:12:52.69@0:
    2020.06.04-18:12:52.69@0: eip=0x08070dbe eflags=0x00010202
    2020.06.04-18:12:52.69@0: edi=0x7fc6e084 esi=0x08130a58
ebp=0x7fc6e008 esp=0x7fc6dfd0
    2020.06.04-18:12:52.69@0: eax=0x081164c4 ebx=0x776fcaf0
ecx=0x0811814c edx=0x00000001
    2020.06.04-18:12:52.69@0:
    2020.06.04-18:12:52.69@0: maps:
    2020.06.04-18:12:52.69@0: 08048000-08115000 r-xp 00000000 00:19 99
      /ram/pckg/wireless/nova/bin/wireless
    2020.06.04-18:12:52.69@0: 7749f000-774a1000 r-xp 00000000 00:0c 959
     /lib/libdl-0.9.33.2.so
    2020.06.04-18:12:52.69@0: 774a3000-774d8000 r-xp 00000000 00:0c 964
     /lib/libuClibc-0.9.33.2.so
    2020.06.04-18:12:52.69@0: 774dc000-774f6000 r-xp 00000000 00:0c 960
     /lib/libgcc_s.so.1
    2020.06.04-18:12:52.69@0: 774f7000-77506000 r-xp 00000000 00:0c 944
     /lib/libuc++.so
    2020.06.04-18:12:52.69@0: 77507000-77664000 r-xp 00000000 00:0c 954
     /lib/libcrypto.so.1.0.0
    2020.06.04-18:12:52.69@0: 77674000-776bf000 r-xp 00000000 00:0c 956
     /lib/libssl.so.1.0.0
    2020.06.04-18:12:52.69@0: 776c3000-776cd000 r-xp 00000000 00:0c 961
     /lib/libm-0.9.33.2.so
    2020.06.04-18:12:52.69@0: 776cf000-776ec000 r-xp 00000000 00:0c 947
     /lib/libucrypto.so
    2020.06.04-18:12:52.69@0: 776ed000-776f3000 r-xp 00000000 00:0c 951
     /lib/liburadius.so
    2020.06.04-18:12:52.69@0: 776f4000-776fc000 r-xp 00000000 00:0c 950
     /lib/libubox.so
    2020.06.04-18:12:52.69@0: 776fd000-77749000 r-xp 00000000 00:0c 946
     /lib/libumsg.so
    2020.06.04-18:12:52.69@0: 7774f000-77756000 r-xp 00000000 00:0c 958
     /lib/ld-uClibc-0.9.33.2.so
    2020.06.04-18:12:52.69@0:
    2020.06.04-18:12:52.69@0: stack: 0x7fc6f000 - 0x7fc6dfd0
    2020.06.04-18:12:52.69@0: c4 64 11 08 07 c8 0f 08 f0 f0 10 08 f0 f0
10 08 28 fe 12 08 84 e0 c6 7f 08 e0 c6 7f 63 3d 06 08
    2020.06.04-18:12:52.69@0: 0c 00 00 00 00 00 00 00 18 e0 c6 7f f0 ca
6f 77 58 0a 13 08 84 e0 c6 7f 38 e0 c6 7f 7c 7a 6f 77
    2020.06.04-18:12:52.69@0:
    2020.06.04-18:12:52.69@0: code: 0x8070dbe
    2020.06.04-18:12:52.69@0: ff 05 00 00 00 00 83 c4 10 53 8b 46 08 0f
b6 40

This vulnerability was initially found in stable 6.46.3, 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
```