Re: Two vulnerabilities found in MikroTik's RouterOS

From: Q C <cq674350529 () gmail com>
Date: Tue, 4 May 2021 15:58:31 +0800

```
[Update 2021/05/04] CVE-2020-20212 and CVE-2020-20211 have been
assigned to these two vulnerabilities.


CVE-2020-20212: Mikrotik RouterOs 6.44.5 (long-term tree) suffers from
a memory corruption vulnerability in the /nova/bin/console process. An
authenticated remote attacker can cause a Denial of Service (NULL
pointer dereference)


CVE-2020-20211: Mikrotik RouterOs 6.44.5 (long-term tree) suffers from
an assertion failure vulnerability in the /nova/bin/console 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4月14日周二 下午6:29写道:

> ```
> [Update 2020/04/14] The latest stable release tree 6.46.5 still suffers
> from these two vulnerabilities.
>
> Details
> =======
>
> Product: MikroTik's RouterOS
> Affected Versions: through 6.46.5 (stable release tree)
> Fixed Versions: -
> Vendor URL: https://mikrotik.com/
> Vendor Status: not fix yet
> CVE: -
> Credit: Qian Chen(@cq674350529) of Qihoo 360 Nirvan Team
>
> Poc
> =======
> The following pocs are based on the tool routeros (
> https://github.com/tenable/routeros)
>
> 1) memory corruption in console process
>
>     WinboxMessage msg;
>     msg.set_to(48, 4);
>     msg.set_command(0xfe0005);
>     msg.add_u32(0xfe000c, -1);
>     msg.add_u32(9, 9);
>
> 2) assertion failure in console process
>
>     WinboxMessage msg;
>     msg.set_to(48, 4);
>     msg.set_command(0xfe0005);
>     msg.add_u32(0xfe0001, 0);
>
> Disclosure timeline
> =======
> 2019/08/23    reported the 2nd issue to the vendor
> 2019/08/26    reported the 1st issue to the vendor
> 2019/08/28    vendor reproduced the 1st issue and will fix it as soon as
> possible
> 2019/08/30    vendor reproduced the 2nd issue and will fix it as soon as
> possible
> 2019/12/02    notified the vendor the 1st issue still exists in version
> 6.44.6 (2nd issue fixed)
> 2020/01/06    no response from the vendor, and did the initial disclosure
> 2020/04/14    re-tested these two issues against the stable 6.46.5, and
> updated the disclosure
> ```

Q C <cq674350529 () gmail com> 于2020年1月6日周一 下午7:32写道:

> ```
> Advisory: two vulnerabilities found in MikroTik's RouterOS
>
>
> Details
> =======
>
> Product: MikroTik's RouterOS
> Affected Versions: before 6.44.6 (Long-term release tree)
> Fixed Versions: 6.44.6 (Long-term release tree)
> 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 two vulnerabilities were tested only against the MikroTik RouterOS
> long-term release tree when found. Maybe other release trees also suffer
> from these issues.
>
> 1. The console process suffers from a memory corruption issue.
> An authenticated remote user can crash the console process due to a NULL
> pointer reference by sending a crafted packet.
>
> 2. The console process suffers from an assertion failure issue. There is
> a reachable assertion in the console process. An authenticated remote user
> can crash the console process duo to assertion failure by sending a crafted
> packet.
>
> Solution
> ========
> ```

> Upgrade to the corresponding latest RouterOS tree version.
>
> References
> ==========
>
> [1] https://mikrotik.com/download/changelogs/long-term-release-tree

By Date By Thread

Current thread:

Re: Two vulnerabilities found in MikroTik's RouterOS *Q C (May 04)*
<Possible follow-ups>
Re: Two vulnerabilities found in MikroTik's RouterOS *Q C (May 04)*
Re: Two vulnerabilities found in MikroTik's RouterOS *Q C (May 04)*
Re: Two vulnerabilities found in MikroTik's RouterOS *Q C (May 07)*