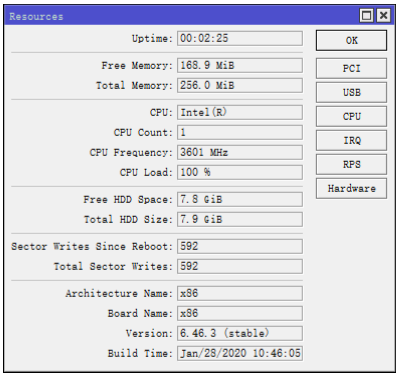
CVE-2020-20248

Description

The `memtest` process suffers from an uncontrolled resource consumption vulnerability. By sending a crafted packet, an authenticated remote user can cause a high cpu load, which may make the device respond slowly or unable to respond.

When testing the proof of concept on an x86 RouterOS VM, this vulnerability will consume all the memory, thus causing the whole system to reboot finally.

Against stable `6.46.3` , the poc resulted in the high cpu load on the device.



```
                Uptime: 00:02:25

           Free Memory: 168.9 MiB
          Total Memory: 256.0 MiB

                   CPU: Intel(R)
             CPU Count: 1
         CPU Frequency: 3601 MHz
              CPU Load: 100 %

        Free HDD Space: 7.8 GiB
        Total HDD Size: 7.9 GiB

Sector Writes Since Reboot: 592
   Total Sector Writes: 592

     Architecture Name: x86
            Board Name: x86
               Version: 6.46.3 (stable)
            Build Time: Jan/28/2020 10:46:05
```

Affected Version

This vulnerability was initially found in stable `6.46.3` , and was fixed in stable `6.47` .

Timeline

- 2020/04/20 - reported the vulnerability to the vendor
- 2020/04/23 - the vendor reproduced and confirmed the vulnerability
- 2021/05/04 - CVE was assigned