Talos Vulnerability Report

TALOS-2020-1115

NZXT CAM WinRing0x64 driver IRP 0x9c402084 information disclosure vulnerability

DECEMBER 16, 2020

CVE NUMBER

CVE-2020-13518

Summary

An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c402084 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.

Tested Versions

NZXT CAM 4.8.0

Product URLs

https://www.nzxt.com/camapp

CVSSv3 Score

6.5 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE

CWE-269 - Improper Privilege Management

Details

NZXT CAM is software designed as an all-in-one solution for computer hardware monitoring and performance. The software monitors fan speeds, CPU temperatures, network and RAM usage, as well as CPU/GPU frequencies for overclocking. It also has features for in-game overlays to track PC performance. The software also has an inventory for all devices that are installed on the PC at any given time.

The WinRing0x64 driver exists so that the NZXT CAM software can have access to the Windows Kernel as well as elevated privileges required to talk to PCI devices as well as making CPU/GPU configuration changes. This driver creates `\Device\WinRing0_1_2_0` that is accessible to any user on the system and this driver is used for all elevated tasks.

Using the IRP 0x9c402084 gives a low privilege user direct access to the `rdmsr` instruction that is completely unrestrained which allows reading of any MSR on the system. This access could be used for leak sensitive information about the processor.

```
00011468  8b09              mov     ecx, dword [rcx]
0001146a  0f32              rdmsr
0001146c  48c1e220          shl     rdx, 0x20
00011470  480bc2            or      rax, rdx
00011473  498900            mov     qword [r8], rax
00011476  488b442428        mov     rax, qword [rsp+0x28 {arg5}]
0001147b  c70008000000      mov     dword [rax], 0x8
00011481  33c0              xor     eax, eax  {0x0}
00011483  eb0d              jmp     0x11492
```

Exploit Proof of Concept

This proof of concept reads the MSR 0xC000_0080 which is the Extended Feature Enable MSR (Core::X86::Msr::EFER)

```
[+] Getting Device Driver Handle
                [+] Device Name: \\.\WinRing0_1_2_0
                [+] Device Handle: 0x94
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x0000015D071C3F50
                        [+] Allocation Size: 0x10
                [+] Preparing Buffer Memory Layout
C0000080 00000000 00000000 00000000 <- MSR Being Read
00004D01 00000000 00000000 00000000 <- MSR Value
```

Timeline

2020-07-17 - Vendor Disclosure
2020-08-10 - Vendor acknowledged; Talos issued copy of reports
2020-11-30 - Public Release

CREDIT

Discovered by Carl Hurd of Cisco Talos.