Talos Vulnerability Report

TALOS-2020-1116

NZXT CAM WinRing0x64 driver IRP 0x9c402088 privilege escalation vulnerability

DECEMBER 16, 2020

CVE NUMBER

CVE-2020-13519

Summary

A privilege escalation vulnerability exists in the WinRing0x64 Driver IRP 0x9c402088 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. 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

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

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 0x9c402088 gives a low privilege user direct access to the `writemsr` instruction that is completely unrestrained which allows writing to any MSR on the system. This access could be used for privilege escalation.

```
0001149c  488bc1            mov     rax, rcx
0001149f  488b5104          mov     rdx, qword [rcx+0x4]
000114a3  48c1ea20          shr     rdx, 0x20
000114a7  8b09              mov     ecx, dword [rcx]
000114a9  8b4004            mov     eax, dword [rax+0x4]
000114ac  0f30              wrmsr
000114ae  488b442428        mov     rax, qword [rsp+0x28 {arg2}]
000114b3  832000            and     dword [rax], 0x0
000114b6  33c0              xor     eax, eax  {0x0}
000114b8  eb0d              jmp     0x114c7
```

Exploit Proof of Concept

This proof of concept the resetting of the MSR 0x10 which is the time stamp counter, with both the initial value and end value being displayed

```
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\WinRing0_1_2_0
                [+] Device Handle: 0x8C
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x0000016B81E83F50
                        [+] Allocation Size: 0x10
                [+] Preparing Buffer Memory Layout
00000010 00000000 00000000 00000000 <- MSR Read
6A1D49D1 00006B7E 00000000 00000000 <- MSR Value
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\WinRing0_1_2_0
                [+] Device Handle: 0x98
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x0000016B81E85EC0
                        [+] Allocation Size: 0x10
                [+] Preparing Buffer Memory Layout
00000010 00000000 00000000 00000000 <- MSR Written
00000000 00000000 00000000 00000000 <- Value Written
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\WinRing0_1_2_0
                [+] Device Handle: 0x9C
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x0000016B81E83F50
                        [+] Allocation Size: 0x10
                [+] Preparing Buffer Memory Layout
00000010 00000000 00000000 00000000 <- MSR Read
003698BA 00000000 00000000 00000000 <- MSR Value
```

Timeline

2020-07-17 - Vendor Disclosure

2020-08-10 - Vendor acknowledged; Talos issued copy of reports

2020-12-16 - Public Release

CREDIT

Discovered by Carl Hurd of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1115

NEXT REPORT

TALOS-2020-1135