Talos Vulnerability Report

TALOS-2020-1113

NZXT CAM WinRing0x64 driver IRP 0x9c406144 information disclosure vulnerability

DECEMBER 16, 2020

CVE NUMBER

CVE-2020-13516

Summary

An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c406144 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 0x9c406144 gives a low privilege user direct access to the `HalGetBusDataByOffset` function. `HalGetBusDataByOffset` can be used to query information from the I/O busses which gives an unprivileged user the ability to directly query information from USB and PCI devices. This access could be used for leak sensitive information.

```
                  // Here we know we have an IRP_MJ_DEVICE_CONTROL packet
0001111e          uint64_t IoControlCode = zx.q(rdx->__offset(0x18).d)
00011127          IoControlCode:0.d - 0x9c4060d4
00011127          bool cond:1_1 = IoControlCode:0.d == 0x9c4060d4
00011127          int64_t rax_1
00011127          if (IoControlCode:0.d u> 0x9c4060d4)
00011346              if (IoControlCode:0.d != 0x9c406104)
00011346                  int64_t var_18
00011346                  if (IoControlCode:0.d == 0x9c406144)
00011346                      uint64_t rbp_1 = zx.q(rdx->InputBufferLength)
00011349                      int32_t* r9_3 = *(Irp + 0x18)
0001134d                      if (rdx->Type3InputBuffer:0.d != 8)
0001134d                          goto label_11306
0001134f                      uint64_t rcx_8 = zx.q(*r9_3)
0001137b                      var_18:0.d = *(r9_3 + 4)
00011380                      int64_t rax_15 = HalGetBusDataByOffset(4, zx.q(zx.d(zx.q(rcx_8:0.d u>> 8):0.b)), zx.q(((rcx_8:0.d u>> 3) &
0x1f) | ((rcx_8:0.d & 7) << 5)), r9_3, var_18, rbp_1:0.d)
0001138a                      if (rax_15:0.d == 0)
0001138a                          rbx = 0xe0000001
000113ab  label_113ab:
000113ab                          *rdi = 0
000113ae                          goto completeRequest
```

Exploit Proof of Concept

This proof of concept iterates through every possible bus addresses and dumps all of the PCI and USB devices on the I/O busses for the system.

```
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\WinRing0_1_2_0
                [+] Device Handle: 0x88
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x000002387B318FB0
                        [+] Allocation Size: 0x10
                [+] Preparing Buffer Memory Layout
Vendor ID : 1022
Device ID : 8010

Vendor ID : 1022
Device ID : 8210

Vendor ID : 1022
Device ID : 8310

Vendor ID : 1022
Device ID : 8310

Vendor ID : 1022
Device ID : 8210...[output truncated]
```

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-2020-1112

NEXT REPORT

TALOS-2020-1114