Talos Vulnerability Report

TALOS-2020-1111

NZXT CAM WinRing0x64 Driver Privileged I/O Write IRPs Privilege Escalation Vulnerability

DECEMBER 16, 2020

CVE NUMBER

CVE-2020-13512, CVE-2020-13513, CVE-2020-13514

Summary

A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs 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.

CVE-2020-13512 - IRP 0x9c40a0d8 - OUT Byte

Using the IRP 0x9c40a0d8 gives a low privilege user direct access to the `OUT` instruction that is completely unrestrained at an elevated privilege level. This allows a low privilege user to write data to the processor I/O ports. This IRP writes only a single byte to the specific processor I/O port. This access could be used for privilege escalation.

```
00011339                if (IoControlCode:0.d == 0x9c40a0d8)
00011339                    IoControlCode:0.b = *(rcx_7 + 4)
0001133c                    unimplemented  {out dx, al}
0001133d                    goto rbx0CompleteRequest
```

CVE-2020-13513 - IRP 0x9c40a0dc - OUT Word

Using the IRP 0x9c40a0dc gives a low privilege user direct access to the `OUT` instruction that is completely unrestrained at an elevated privilege level. This allows a low privilege user to write data to the processor I/O ports. This IRP writes two bytes (1 word) to the specific processor I/O port. This access could be used for privilege escalation.

```
0001132e                if (IoControlCode:0.d == 0x9c40a0dc)
0001132e                    *(rcx_7 + 4)
00011332                    unimplemented  {out dx, ax}
00011334                    goto rbx0CompleteRequest
```

CVE-2020-13514 - IRP 0x9c40a0e0 - OUT Dword

Using the IRP 0x9c40a0e0 gives a low privilege user direct access to the `OUT` instruction that is completely unrestrained at an elevated privilege level. This allows a low privilege user to write data to the processor I/O ports. This IRP writes four bytes (one dword) to the specific processor I/O port. This access could be used for privilege escalation.

```
00011323                if (IoControlCode:0.d != 0x9c40a0e0)
00011323                    goto label_11306
00011325                *(rcx_7 + 4)
00011328                unimplemented  {out dx, eax}
00011329                goto rbx0CompleteRequest
```

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.
