

Talos Vulnerability Report

TALOS-2021-1255

IOBit Advanced SystemCare Ultimate Privileged I/O Read vulnerabilities

JULY 7, 2021

CVE NUMBER

CVE-2021-21790, CVE-2021-21791, CVE-2021-21792

Summary

An information disclosure vulnerability exists in the way IObit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. A local attacker can craft a malicious IRP to trigger this vulnerability.

Tested Versions

IObit Advanced SystemCare Ultimate 14.2.0.220

Product URLs

<https://www.iobit.com/>

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-782 - Exposed IOCTL with Insufficient Access Control

Details

IObit Advanced SystemCare Ultimate provides a solution for keeping track of running services, processes that are using a large amount of memory, software updates, and the ability to update drivers to latest versions.

Advanced SystemCare also provides a monitoring driver to help facilitate its tasks. This driver creates \Device\IOBIT_WinRing0_1_3_0 which is readable and writable to everyone. The driver also provides a callback for handling IRP_MJ_DEVICE_CONTROL requests to the driver.

The driver used in this analysis is below:

Monitor_win10_x64.sys e4a7da2cf59a4a21fc42b611df1d59cae75051925a7ddf42bf216cc1a026eadb

CVE-2021-21790 - Exposed IN byte

During IOCTL 0x9c4060cc, the first int passed in the input buffer is the device port to read from via the IN instruction. The IN instruction can read one byte from the given I/O device, potentially leaking sensitive device data to unprivileged users.

```
Monitor_win10_x64.sys+0x11189

first_u32 = *(_DWORD *)input_buffer;
switch ( ioctl )
{
case 0x9C4060CC:
    out_byte = __inbyte(first_u32);
    *(_BYTE *)input_buffer = out_byte;
    goto LABEL_28;
```

CVE-2021-21791 - Exposed IN word

During IOCTL 0x9c4060d0, the first int passed in the input buffer is the device port to read from via the IN instruction. The IN instruction can read two bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users.

```
Monitor_win10_x64.sys+0x11189

first_u32 = *(_DWORD *)input_buffer;
switch ( ioctl )
{
...
case 0x9C4060D0:
    out_word = __inword(first_u32);
    *(_WORD *)input_buffer = out_word;
    goto LABEL_28;
```

CVE-2021-21792 - Exposed IN dword

During IOCTL 0x9c4060d4, the first int passed in the input buffer is the device port to read from via the IN instruction. The IN instruction can read four bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users.

```
Monitor_win10_x64.sys+0x11189

first_u32 = *(_DWORD *)input_buffer;
switch ( ioctl )
{
...
    case 0x9C4060D4:
        out_dword = __indword(first_u32);
        *(_DWORD *)input_buffer = out_dword;
LABEL_28:
        *(_DWORD *)iostatus_info = v8;
        goto LABEL_64;
```

Exploit Proof of Concept

In combination with the exposed OUT instruction, an unprivileged user can access PCI devices on the system.

```
Opening Device
File Handle: 0xa0
Dumping PCI devices
Device: 0x1237 Vendor: 0x8086
Device: 0x7000 Vendor: 0x8086
Device: 0x100e Vendor: 0x80ee
Device: 0x2668 Vendor: 0x8086
Device: 0x003f Vendor: 0x106b
Device: 0x7113 Vendor: 0x8086
Device: 0x2829 Vendor: 0x8086
```

Timeline

2021-02-17 - Initial contact
2021-02-23 - Vendor disclosure
2021-03-10 - Follow up with vendor
2021-04-30 - 2nd follow up with vendor
2021-05-17 - 3rd follow up with vendor
2021-06-27 - Final follow up with vendor
2021-07-07 - Public release

CREDIT

Discovered by Cory Duplantis of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2021-1254

TALOS-2021-1281
