Talos Vulnerability Report

TALOS-2021-1254

IOBit Advanced SystemCare ultimate privileged I/O write vulnerabilities

JULY 7, 2021

CVE NUMBER

CVE-2021-21787, CVE-2021-21788,CVE-2021-21789

Summary

A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. A specially crafted I/O request packet (IRP) can lead to privileged writes which can result in elevation of privileges of the current user. A local attacker can send 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

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

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 faciltate 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-2021-21787 - Exposed OUT byte

During IOCTL `0x9c40a0d8`, the first `dword` passed in the input buffer is the device port to write to and the `byte` at offset 4 is the value to write via the `OUT` instruction. The `OUT` instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users.

```
Monitor_win10_x64.sys+0x11310

u32_at_0 = *(_DWORD *)input_buffer_1;
  switch ( ioctl )
  {
    case 0x9C40A0D8:
      __outbyte(u32_at_0, *((_BYTE *)input_buffer_1 + 4));
      goto LABEL_64;
```

CVE-2021-21788 - Exposed OUT word

During IOCTL `0x9c40a0dc`, the first `dword` passed in the input buffer is the device port to write to and the `word` at offset 4 is the value to write via the `OUT` instruction. The `OUT` instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users.

```
Monitor_win10_x64.sys+0x11310

u32_at_0 = *(_DWORD *)input_buffer_1;
  switch ( ioctl )
  {
  ...
        case 0x9C40A0DC:
          __outword(u32_at_0, *((_WORD *)input_buffer_1 + 2));
          goto LABEL_64;
```

CVE-2021-21789 - Exposed OUT dword

During IOCTL `0x9c40a0e0`, the first `dword` passed in the input buffer is the device port to write to and the `dword` at offset 4 is the value to write via the `OUT` instruction. The `OUT` instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users.

```
Monitor_win10_x64.sys+0x11310

u32_at_0 = *(_DWORD *)input_buffer_1;
  switch ( ioctl )
  {
  ...
    case 0x9C40A0E0:
          __outdword(u32_at_0, *((_DWORD *)input_buffer_1 + 1));
          goto LABEL_64;
```

Exploit Proof of Concept

In combination with the exposed `IN` 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

2021-03-10 - 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.