Talos Vulnerability Report

TALOS-2021-1252

IOBit Advanced SystemCare Ultimate exposed IOCTL 0x9c40a148 vulnerability

JULY 7, 2021

CVE NUMBER

CVE-2021-21785

Summary

An information disclosure vulnerability exists in the IOCTL 0x9c40a148 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to a disclosure of sensitive information. An 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

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 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

During IOCTL `0x9c40a148`, unprivileged user controlled data is passed to the `HalSetBusDataByOffset` function. This data is not constrained, giving the unprivileged user the ability to read any I/O device’s configuration and device specific registers. The reading of this information can lead to the disclosure of sensitive information to the user.

```
Monitor_win10_x64.sys+0x112ad

case 0x9C40A148:
  v14 = v4->Parameters.DeviceIoControl.InputBufferLength;
  if ( v14 < 8 )
  {
    v5 = 0xC000000D;
    goto LABEL_65;
  }
  input_buffer_3 = a2->AssociatedIrp.SystemBuffer;
  *(_DWORD *)iostatus_info = 0;
  v5 = v14 - 8 != HalSetBusDataByOffset(
                    PCIConfiguration,
                    (unsigned __int8)BYTE1(*(_DWORD *)input_buffer_3),
                    (32 * (*(_DWORD *)input_buffer_3 & 7)) | ((unsigned __int8)*(_DWORD *)input_buffer_3 >> 3),
                    (char *)input_buffer_3 + 8,
                    *((_DWORD *)input_buffer_3 + 1),
                    v14 - 8) ? 0xE0000003 : 0;
  break;
```

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.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1234

NEXT REPORT

TALOS-2021-1253