Talos Vulnerability Report

TALOS-2021-1253

IOBit Advanced SystemCare Ultimate exposed IOCTL 0x9c406144 vulnerability

JULY 7, 2021

CVE NUMBER

CVE-2021-21786

Summary

A privilege escalation vulnerability exists in the IOCTL 0x9c406144 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to increased privileges. 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

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

During IOCTL `0x9c406144`, unprivileged user controlled data is passed to the `HalGetBusDataByOffset` function. This data is not constrained, giving the unprivileged user the ability to change I/O device configuration and device specific registers. The modification of this sensitive data can lead to the unprivileged user elevating their privileges.

```
Monitor_win10_x64.sys+0x11349

case 0x9C406144:
  input_buffer_2 = a2->AssociatedIrp.SystemBuffer;
  v20 = HalGetBusDataByOffset(
          PCIConfiguration,
          (unsigned __int8)BYTE1(*(_DWORD *)input_buffer_2),
          (32 * (*(_DWORD *)input_buffer_2 & 7)) | ((unsigned __int8)*(_DWORD *)input_buffer_2 >> 3),
          input_buffer_2,
          *((_DWORD *)input_buffer_2 + 1),
          v4->Parameters.DeviceIoControl.OutputBufferLength);
  if ( v20 )
  {
    if ( output_buffer_len == 2 || v20 != 2 )
    {
      if ( output_buffer_len == v20 )
      {
        *(_DWORD *)iostatus_info = output_buffer_len;
        goto LABEL_64;
```

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.