

master Kernel-exploits / AscRegistryFilter.sys /

GREENSHADE commit ... on Jun 15, 2020 History

| | |
|-------------------|-------------|
| .. | |
| images | 2 years ago |
| 0x8001E000-BSOD.c | 2 years ago |
| README.md | 2 years ago |

README.md

Advanced SystemCare 13.2 Kernel vulnerabilities

BSOD POC's for (Advanced SystemCare 13.2) AscRegistryFilter.sys (CVE-2020-10234)

About

- Description:**
Advanced SystemCare 13.2 is a anti-virus/threat detectiong software provided by IObit. The version 13.2.0 includes multiple drivers, one of which, (AscRegistryFilter.sys) is prone to multiple vulnerabilities.

CVE-2020-10234

- Description:**
AscRegistryFilter Windows x86 Kernel Driver allows unprivileged user's unrestricted access while sending IOCTL's to the associated device driver. While utilizing DeviceIoControl() , if the user provides a NULL entry for the dwIoControlCode parameter. It will result in a BSOD ak.k.a Kernel-Panic.
- POC exploit:**
An unprivileged user can send one of the listed IOCTL's found below. These IOCTL codes can be found in the dispatch_function while reverse-engineering the driver with IDA Pro. The BSOD POC in this repository uses the first IOCTL code 0x8001E000 . Bound with a NULL buffer.

| Address | IOCTL Code | Device | | | Function | Method | Access |
|---------|------------|-----------|--------|-------|-----------------|--------|--|
| 0x11847 | 0x8001E000 | <UNKNOWN> | 0x8001 | 0x800 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11852 | 0x8001E004 | <UNKNOWN> | 0x8001 | 0x801 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x1185D | 0x8001E008 | <UNKNOWN> | 0x8001 | 0x802 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11868 | 0x8001E00C | <UNKNOWN> | 0x8001 | 0x803 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11873 | 0x8001E010 | <UNKNOWN> | 0x8001 | 0x804 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x1187E | 0x8001E014 | <UNKNOWN> | 0x8001 | 0x805 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11809 | 0x8001E020 | <UNKNOWN> | 0x8001 | 0x808 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11814 | 0x8001E024 | <UNKNOWN> | 0x8001 | 0x809 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x1181F | 0x8001E040 | <UNKNOWN> | 0x8001 | 0x810 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x1182A | 0x8001E044 | <UNKNOWN> | 0x8001 | 0x811 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |
| 0x11835 | 0x8001E048 | <UNKNOWN> | 0x8001 | 0x812 | METHOD_BUFFERED | 0 | FILE_READ_ACCESS FILE_WRITE_ACCESS (3) |

Driver Device names:

\\DosDevices\\AscRegistryFilter
\\Device\\AscRegistryFilter

A problem has been detected and windows has been shut down to prevent damage to your computer.

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to be sure you have adequate disk space. If a driver is identified in the Stop message, disable the driver or check with the manufacturer for driver updates. Try changing video adapters.

Check with your hardware vendor for any BIOS updates. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup options, and then select Safe Mode.

Technical information:

*** STOP: 0x0000008E (0xC0000005, 0x82659230, 0xA3769A2C, 0x00000000)

collecting data for crash dump ...
initializing disk for crash dump ...
beginning dump of physical memory.
dumping physical memory to disk: 20

- **Disclosure timeline:**

1. Mar 8, 2020 - Contacted vendor via support email
2. Nothing happened