master Kernel-exploits / MaxProc64.sys /

GREENSHADE commit ... on Jun 15, 2020 History

..

README.md	2 years ago
bsod.png	2 years ago
poc.cpp	2 years ago
poc2.cpp	2 years ago

README.md

CVE-2020-12122

In Max Secure Max Spyware Detector 1.0.0.044, the driver file (MaxProc64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtls 0x2200019. This also extends to the various other products from Max Secure which include this driver.

Data passed to this IOCTL that is invalid results in a BSOD.

Edit : It seems like @hFireF0X discovered this around the same time as I, my CVE request took months, and it doesn't look like they (or anyone) requested one.

That makes this like a 1/3rd 0day discovery, but within this repo is a POC for BSOD.

```
# Exploit Title: Max Secure Max SPyware Detector (MaxProc64.sys) IOCTL DOS
# Google Dork: N/A
# Date: 04/10/2020
# Exploit Author: FULLSHADE
# Vendor Homepage: https://www.maxpcsecure.com
# Software Link: http://www.maxpcsecure.com/MaxSDDM.exe
# Version: 1.0.0.044
# Tested on: Windows 7
# CVE : CVE-2020-12122
```

NIST: NVD

Base Score: 7.8 HIGH

Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H