CVE-2018-6319

Blue Screen of Death in Sophos Tester Tool

By

Valthek

The Sophos company tool called Sophos Tester tool in its versions 3.2.0.7 and 3.2.0.12 (possibly in some previous or later that I could not obtain or check also keep in mind the exploit).

Version 3.2.0.7 has a compilation date of May 29, 2017 and 3.2.0.12 of October 10, 2017.

Both versions can be found in VirusTotal and possibly in other more public sites over the Internet.

3.2.0.7 -> https://www.virustotal.com/#/file/a739c3b087e04bb5beddf08ce9a056b1af989e4b4d1add8eea290cbec475da0f/detection

3.2.0.12 -> https://www.virustotal.com/#/file/6aafa205568e9ce6ac6d56ebf55beb254e835691c66f9b794d3cc860166274f4/detection

In its first execution, the tool creates a signed driver (with a valid signature at the current date for all operating systems) and a dynamic library in the "System32" directory, the library or in the WoW folder in the case of a 64bit operating system with a 32bit tool.

The controller has the name "tester86.sys" if the operating system is 32 bits or "tester64.sys" in the case of 64 bits. The dynamic library has the name "tester86.dll".

While the driver and library are encrypted in the tool, they can be obtained simply by running and installing the application and get them from the folders.

- ## USE OF THE TOOL

The tool is used to test existing exploits, emulated ransomware, code integrity, etc.

For this you can use the application itself or another application installed on the system, for example, a PDF viewer.

After carrying out the relevant verification, the application returns whether the test could be performed or not.

- ## CVE-2018-6319

However, the controller is not exempt from a serious failure. When the controller starts at the request of the application, it performs a series of operations to check which processes are loaded, if it is the same, etc.

In order to start performing the activity that the user chose, he has to put a flag 1, which by default is 0.

For this, the application sends a control code through the "DeviceIoControl" API, with the control code in hexadecimal 0x222000. The function responsible for receiving the command proceeds to check if the buffer contributed to this function has at least one byte since the application sends a simple byte to indicate that the flag must be set to 1.

The problem occurs because it has no verification that the memory address to be checked is accessible or actually exists, so if a null pointer or a non-existent address is sent in the kernel,

an automatic **Blue Screen Of Death** will be produced. .

```
_check_arguments:                       ; CODE XREF: SophosIOCTLControlerDeviceIoIRP+12↑j
                mov     eax, [esi+0Ch]
                cmp     byte ptr [eax], 0
                jz      short _clear_vars_to_zeroe
                call    ds:PsGetCurrentProcessId
                mov     SophosGetCurrentProcessIDValueVar, eax
                mov     SophosHaveTheOrGetCurrentProcessIdFlag, 1
                jmp     short _clear_edi
```

This also occurs because no control block is being used that can handle the exception.

- ## POSSIBLE USES OF THE EXPLOIT

Taking into account that the driver can be obtained from the "drivers" folder of the "System32" directory and that the driver does not receive any special arguments when loaded by the official application, it can be picked up and used in any other application.

That application would only have to create the file in a directory with write permissions, and having administrator permissions create a kernel mode service through SC Manager to boot with the system.

Once the service is started and the running controller is creating a symbolic link with the name "testerdrv", which can be accessed without problem using the CreateFile API and after obtaining its driver use "DeviceIoControl" with a wrong address and the indicated code previously to produce the **Blue Screen Of Death**.

A malicious application that had persistence could do this in each boot leaving a system in a continuous restart after receiving a Blue Screen Of Death since Windows has by default activated the option of autoreinicio in those cases. This could produce a Deniego of Service of the machine itself, if the user is a normal user who does not know how to stop the application or stop the service.

With this PDF a simple POC is provided without persistence but it shows how in a system with the application in execution that attack can be made.