

corelight / CVE-2021-1675

Public

Notifications

Fork 4

Star 9

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

master



<> Code

20 Commits		
scripts		
testing		
README.md		
suricata.rules		
zkg.meta		

README

PrintNightmare (CVE-2021-1675)

This Zeek script detects successful `RpcAddPrinterDriver{,Ex}` DCE RPC events, which are required to successfully exploit the vulnerability. Tests are based on exploit PCAP from [Lares Lab](#). Tested with Zeek versions `3.0.2` and `4.0.1`.

Notices

- `Printer_Driver_Changed_Successfully` indicates the printer driver was changed successfully.

Suricata

We have also provided [Suricata rules](#) to detect the DCE RPC commands used in this exploit. These can be either loaded into a Corelight appliance, or run directly with Suricata. These rules fire a lot on larger networks and may be sufficiently noisy so as not to be useful. Please use with caution. We have kept them here in case they are useful in other networks. In our opinion, the Zeek package is more robust against noise.

The output of running Suricata with the provided ruleset is shown below:

```
$ suricata -r testing/Traces/PrintNightmare.pcap -S suricata.rules
8/7/2021 -- 10:54:57 - <Notice> - This is Suricata version 6.0.3 RELI
8/7/2021 -- 10:54:57 - <Warning> - [ERRCODE: SC_WARN_ERSPAN_CONFIG(3:
8/7/2021 -- 10:54:57 - <Notice> - all 17 packet processing threads,
8/7/2021 -- 10:54:57 - <Notice> - Signal Received. Stopping engine.
8/7/2021 -- 10:54:57 - <Notice> - Pcap-file module read 1 files, 53 |

$ cat fast.log
07/02/2021-08:11:57.785982  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.824060  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.848240  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.848240  [**] [1:3000008:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.894097  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.894097  [**] [1:3000008:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.959051  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:11:57.959051  [**] [1:3000008:2] CORELIGHT Possible CVI
07/02/2021-08:11:58.000581  [**] [1:3000007:2] CORELIGHT Possible CVI
```

About

No description, website, or topics provided.

- Readme
- Activity
- Custom properties
- 9 stars
- 11 watching
- 4 forks
- Report repository


Releases


No releases published


Packages

No packages published

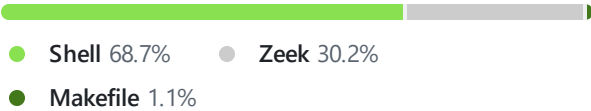
Contributors 3







Languages



```
07/02/2021-08:11:58.000581  [**] [1:3000008:2] CORELIGHT Possible CVI
07/02/2021-08:11:58.007953  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:12:08.520328  [**] [1:3000007:2] CORELIGHT Possible CVI
07/02/2021-08:12:08.520328  [**] [1:3000008:2] CORELIGHT Possible CVI
```

References

- <https://github.com/LaresLLC/CVE-2021-1675>
- <https://github.com/afwu/PrintNightmare>
- <https://github.com/cube0x0/CVE-2021-1675>

