Sign in

corelight / CVE-2021-1675 Public

Notifications Fork 4 Star 9

Code Issues Pull requests Actions Projects Security Insights

master Go to file Code

- 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

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

- ynadji yacin
- benjeems Ben Reardon
- pbcullen Peter Cullen

- `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.pca
8/7/2021 -- 10:54:57 - <Notice> - This is Surica
8/7/2021 -- 10:54:57 - <Warning> - [ERRCODE: SC_
8/7/2021 -- 10:54:57 - <Notice> - all 17 packet
8/7/2021 -- 10:54:57 - <Notice> - Signal Receiv
8/7/2021 -- 10:54:57 - <Notice> - Pcap-file mod

$ cat fast.log
07/02/2021-08:11:57.785982  [**] [1:3000007:2] (
07/02/2021-08:11:57.824060  [**] [1:3000007:2] (
07/02/2021-08:11:57.848240  [**] [1:3000007:2] (
07/02/2021-08:11:57.848240  [**] [1:3000008:2] (
07/02/2021-08:11:57.894097  [**] [1:3000007:2] (
07/02/2021-08:11:57.894097  [**] [1:3000008:2] (
07/02/2021-08:11:57.959051  [**] [1:3000007:2] (
07/02/2021-08:11:57.959051  [**] [1:3000008:2] (
07/02/2021-08:11:58.000581  [**] [1:3000007:2] (
07/02/2021-08:11:58.000581  [**] [1:3000008:2] (
07/02/2021-08:11:58.007953  [**] [1:3000007:2] (
07/02/2021-08:12:08.520328  [**] [1:3000007:2] (
07/02/2021-08:12:08.520328  [**] [1:3000008:2] (
```

References

Languages

● Shell 68.7% ● Zeek 30.2%
● Makefile 1.1%

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

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information