zerosum0x0 / CVE-2019-0708

Watch 64 Star 886 Fork 258

Scanner PoC for CVE-2019-0708 RDP RCE vuln

54 commits 1 branch 0 releases 3 contributors Apache-2.0

Branch: master ▾ New pull request Find File Clone or download ▾

zerosum0x0 Update README.md Latest commit `069344c` May 31, 2019

docker	Added a Docker image that builds from source	May 22, 2019
rdesktop-fork-bd6aa6acddf0ba640a4...	Fixed exit code so that it is consistent	May 23, 2019
.gitignore	Initial commit	May 22, 2019
Dockerfile	Added a Docker image that builds from source	May 22, 2019
LICENSE	Initial commit	May 22, 2019
README.md	Update README.md	May 31, 2019
cve_2019_0708_bluekeep.rb	auxiliary/scanner/rdp/cve_2019_0708_bluekeep is in rapid7:master	May 24, 2019
scan_with_docker.py	Exit if there's no hosts to scan	May 23, 2019
screenshot.png	add screenshot	May 22, 2019

README.md

CVE-2019-0708

Unauthenticated CVE-2019-0708 "BlueKeep" Scanner PoC by @JaGoTu and @zerosum0x0.

Technical details: https://zerosum0x0.blogspot.com/2019/05/avoiding-dos-how-bluekeep-scanners-work

Metasploit Module

The Metasploit module has been pulled to rapid7:master.

```
msf5> use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
```

https://github.com/rapid7/metasploit-framework/pull/11869

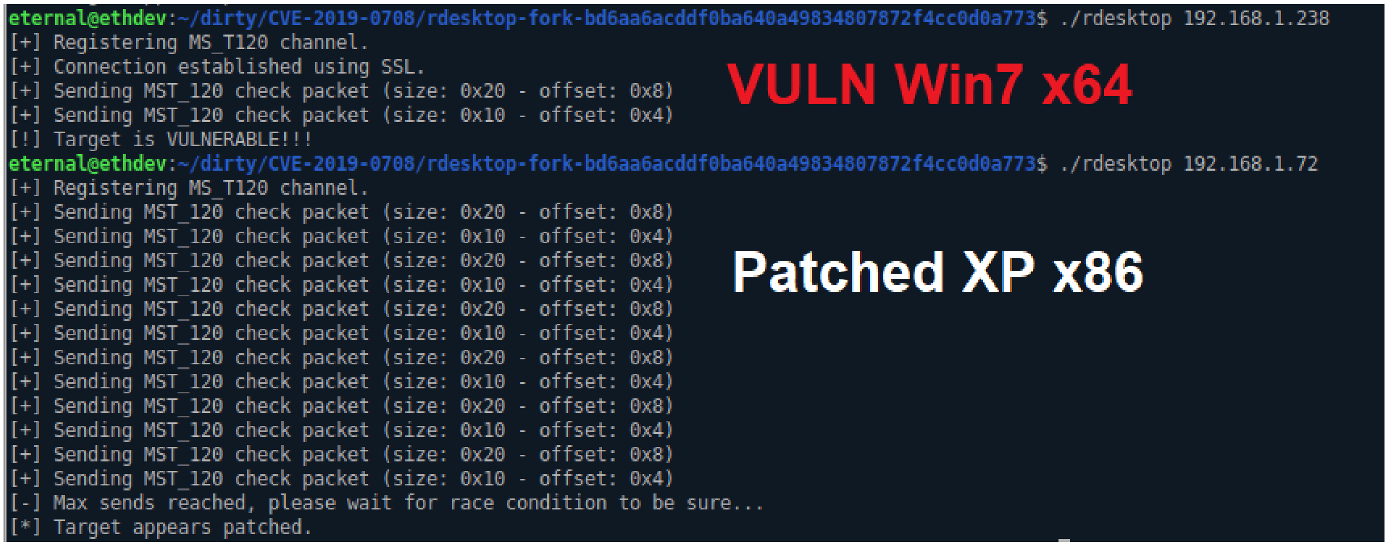
RDPScan

If you're here for the C version of the scanner, check out ErrataRob's fork of this project which trims more fat and makes scanning a large range faster/easier.

https://github.com/robertdavidgraham/rdpscan

In this repo

A scanner fork of rdesktop that can detect if a host is vulnerable to CVE-2019-0708 Microsoft Windows Remote Desktop Services Remote Code Execution vulnerability. It shouldn't cause denial-of-service, but there is never a 100% guarantee across all vulnerable versions of the RDP stack over the years. As it is unauthenticated, the scanner will not have reliable results for NLA hosts (which is a confirmed mitigation).



```
eternal@ethdev:~/dirty/CVE-2019-0708/rdesktop-fork-bd6aa6acddf0ba640a49834807872f4cc0d0a773$ ./rdesktop 192.168.1.238
[+] Registering MS_T120 channel.
[+] Connection established using SSL.
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[!] Target is VULNERABLE!!!
eternal@ethdev:~/dirty/CVE-2019-0708/rdesktop-fork-bd6aa6acddf0ba640a49834807872f4cc0d0a773$ ./rdesktop 192.168.1.72
[+] Registering MS_T120 channel.
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[+] Sending MST_120 check packet (size: 0x20 - offset: 0x8)
[+] Sending MST_120 check packet (size: 0x10 - offset: 0x4)
[-] Max sends reached, please wait for race condition to be sure...
[*] Target appears patched.
```

Building and Running

There is a pre-made rdesktop binary in the repo, but is a normal rdesktop build process:

```
git clone https://github.com/zerosum0x0/CVE-2019-0708.git
cd CVE-2019-0708/rdesktop-fork-bd6aa6acddf0ba640a49834807872f4cc0d0a773/
./bootstrap
./configure --disable-credssp --disable-smartcard
```

```
make
./rdesktop 192.168.1.7:3389
```

s fork of rdesktop is only well supported on an **X11 GUI Linux environment**. Results will vary for other plat Please refer to the normal rdesktop compilation instructions or have a look at how the Docker image is built.

Docker Instructions

You can also build from source using the Dockerfile and then run rdesktop using that image:

```
docker build . -t cve-2019-0708:latest
docker run cve-2019-0708:latest 192.168.1.7:3389
```

To scan a subnet or hosts indexed by Shodan, build the Docker image and run scan_with_docker.py:

```
./scan_with_docker.py 'asn:ASXXXX port:3389'
Not a valid subnet. Trying to use as Shodan search terms ...
Shodan search returned 498 hosts, press enter to start scan
Vulnerable hosts:
x.x.x.x
x.x.x.x
[...]

./scan_with_docker.py 192.168.1.0/24
Vulnerable hosts:
192.168.1.28
192.168.1.30
[...]
```

Is this dangerous?

Small details of the vulnerability have already begun to reach mainstream. This tool does not grant attackers a free ride to a theoretical RCE.

Modifying this PoC to trigger the denial-of-service does lower the bar of entry but will also require some amount of effort. We did not originally offer an explanation of how this scanner works other than to tell the user it seems to be accurate in testing and follows a logical path.

System administrators need tools like this to discover vulnerable hosts. This tool is offered for legal purposes only and to forward the security community's understanding of this vulnerability. As this PoC actively exploits the vulnerability, do not use against targets without prior permission.

Contributors

- JaGoTu
- zerosum0x0
- SUNET

License

rdesktop fork is licensed as GPLv3.

Metasploit module is licensed as Apache 2.0.