

# **[VulnWatch] iDEFENSE Security Advisory 09.13.05: Linksys WRT54G Router Remote Administration Fixed Encryption Key Vulnerability**

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-09/0006.html>

---

*From:* iDEFENSE Labs ([labs-no-reply\\_at\\_idefense.com](mailto:labs-no-reply_at_idefense.com))

*Date:* 09/13/05

Date: Tue, 13 Sep 2005 17:15:35 -0400

To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>, <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>, <[full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)>

Linksys WRT54G Router Remote Administration Fixed Encryption Key  
Vulnerability

iDEFENSE Security Advisory 09.13.05

[www.idefense.com/application/poi/display?id=304&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=304&type=vulnerabilities)

September 13, 2005

## I. BACKGROUND

The Linksys WRT54G is a combination wireless access point, switch and router. More information is available at the following URL:

<http://www.linksys.com/products/product.asp?prid=508>

## II. DESCRIPTION

Remote exploitation of a design error in multiple versions of the firmware for Cisco Systems Inc.'s Linksys WRT54G wireless router may allow unauthenticated modification of the router configuration.

The vulnerability specifically exists in the 'ezconfig.asp' handler of the httpd running on the internal interfaces, including by default the wireless interface. This handler is used by the 'ezSetup' to perform

the initial setup of the router.

```
struct mime_handler mime_handlers[] = {  
  //{ "ezconfig.asp", "text/html", ezc_version, do_apply_ezconfig_post,  
    do_ezconfig_asp, do_auth },  
  /*Modified by Daniel(2004-09-06);*/  
  { "ezconfig.asp", "text/html", ezc_version, do_apply_ezconfig_post,  
    do_ezconfig_asp, NULL },
```

The 'auth()' method for this page does not contain an authentication initialization function. As the authentication initializer (do\_auth) was

removed, no check is made when requesting the page. If the auth\_fail flag was set for any reason, this call will fail. The code which sets the auth\_fail flag is shown below. When the httpd starts, the value of auth\_flag defaults to 0.

```
if (handler->auth) {  
    handler->auth(auth_userid, auth_passwd, auth_realm);  
    auth_fail = 0;  
    if (!auth_check(auth_realm, authorization))  
        auth_fail = 1;  
}
```

The request returns an encrypted version of the configuration information, however the encryption on this data is very weak, it is a simple XOR based encryption, with a fixed 256 byte mask. In order to change the configuration, this key must be known. Once this key is known

and the new configuration data is encrypted with it, and the new data can simply be posted to the httpd, the new configuration will take effect.

### III. ANALYSIS

Successful exploitation of this vulnerability would allow an unauthenticated user the ability to modify the configuration of the affected router, including the password. This could allow firewall rules

to be changed, installation of a new firmware with other features, or denial of service. Exploitation of this vulnerability would require that

an attacker can connect to the web management port of the router. The httpd is running by default but is only accessible via the LAN ports or the WLAN (wireless LAN).

An attacker who can associate with a network running a vulnerable httpd could send an exploit from a wireless device to reset the password on the device and enable the remote management port, allowing continued internet access.

Authentication credentials may be set if another user has attempted to view a page since the router was restarted. An attacker may be able to crash the httpd using another vulnerability, in which case it will restart within 2 minutes, with no authentication details initialized. This would then allow them to exploit the httpd with this vulnerability.

### IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in version 3.01.03 of the firmware of the Linksys WRT54G, and has identified the same code is present in version 3.03.6.

Version 2.04.4 of the WRT54G is confirmed to contain the affected code, however by default it initializes the authentication details, and so requires a password to set the configuration.

## V. WORKAROUND

In order to prevent exposure of this vulnerability from wireless clients, disable wireless access to the web interface:

- \* Connect to the web interface, typically at <http://192.168.1.1/>
- \* Go to the Administration page
- \* Select 'Disable' next to the 'Wireless Access Web'
- \* Click the 'Save Settings' button.

Please note that this will only prevent wireless access, and not access from one of the physical ports. Additionally, other vulnerabilities in the httpd may allow exploitation of the router, even with this setting enabled.

In order to mitigate exposure of the router and internal network to outside attackers, ensure encryption is enabled on the wireless interface. The exact settings to use are dependent on your wireless deployment policies.

## VI. VENDOR RESPONSE

<http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout>

&packedargs=c%3DL\_Download\_C2%26cid%3D1115417109974%26sku%3D1124916802645

&pagename=Linksys%2FCommon%2FVisitorWrapper

## VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

## VIII. DISCLOSURE TIMELINE

06/07/2005 Initial vendor notification  
06/07/2005 Initial vendor response  
09/13/2005 Coordinated public disclosure

## IX. CREDIT

This vulnerability was discovered by Greg MacManus of iDEFENSE Labs.

Get paid for vulnerability research

<http://www.idefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events

<http://labs.idefense.com>

## X. LEGAL NOTICES

Copyright (c) 2005 iDEFENSE, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDEFENSE. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email [customerservice@idefense.com](mailto:customerservice@idefense.com) for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.