

[Full-disclosure] iDEFENSE Security Advisory 09.13.05: Linksys WRT54G 'restore.cgi' Configuration Modification Design Error Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0396.html>

From: iDEFENSE Labs (*labs-no-reply_at_idefense.com*)

Date: 09/13/05

Date: Tue, 13 Sep 2005 17:16:46 -0400

To: <bugtraq@securityfocus.com>, <vulnwatch@vulnwatch.org>, <full-disclosure@lists.grok.org.uk>

Linksys WRT54G 'restore.cgi' Configuration Modification Design Error
Vulnerability

iDEFENSE Security Advisory 09.13.05

www.idefense.com/application/poi/display?id=306&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 the 'restore.cgi' component of Cisco Systems Inc.'s Linksys WRT54G wireless router may allow unauthenticated modification of the router configuration.

The vulnerability specifically exists in the 'POST' method of restore.cgi handler. The httpd running on the internal interfaces, including by default the wireless interface, does not check if authentication has failed until after data supplied by an external user has been processed. The restore.cgi handler allows a user to upload a new configuration into the non-volatile memory of the router. If the user is authenticated, the router will then restart, and the new configuration will be loaded.

If the user is not authenticated, they will receive an error page when they attempt to upload a new configuration without supplying authentication and the router will not reboot. The settings the user

set will be saved, but will not take effect until the next time the router restarts.

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). A mitigating factor is that if the firmware settings are saved by a process on the router before the server is reset, the saved settings will overwrite the settings uploaded by the attacker.

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 access from the Internet.

IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in version 3.01.03 of the firmware of the Linksys WRT54G wireless router, and has identified the same code is present in versions 3.03.6 and 4.00.7. All versions prior to 4.20.7 may be affected.

V. WORKAROUND

To mitigate exposure of the 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

This vulnerability is addressed in firmware version 4.20.7 available for download at:

<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

07/05/2005 Initial vendor notification
07/25/2005 Initial vendor response
09/12/2005 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 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.

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>