

iDEFENSE Security Advisory 09.13.05: Linksys WRT54G 'restore.cgi' Configuration Modification Design Error Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-09/0137.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