

## RE: Serious flaw in Linksys wireless AP password security

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-08/0224.html>

---

**From:** Robert Thompson Jr. (*rthompson\_at\_columbiabank.com*)

**Date:** 08/16/05

Date: Tue, 16 Aug 2005 11:59:15 -0700

To: "Steve Scherf" <steve@moonsoft.com>, <bugtraq@securityfocus.com>

Thank you for the link. I appreciate it.

After reading through it, I am beginning to see where I may have misunderstood what you were getting at.

When I was attempting to get into the router, with WZC set open, and encryption was enabled on my router, but not on my nic, there was no connecting.

And with a wrong key, no connecting.

BUT – one thing that I did not do, was attempt to connect to the router via WZC with the encryption turned ON but with no key supplied. I always had a key loaded should the encryption be enabled.

I will test encryption on with no key when I get home tonight and see what happens. Unfortunately, I will have to flash back down to the 4.50.6 firmware, BUT I'm curious.

Again, thank you for the link...

-----Original Message-----

From: Steve Scherf [mailto:steve@moonsoft.com]

Sent: Tuesday, August 16, 2005 11:00 AM

To: Robert Thompson Jr.

Cc: Steve Scherf; bugtraq@securityfocus.com

Subject: Re: Serious flaw in Linksys wireless AP password security

FYI, the problem I reported has been reproduced over at Broadband Reports:

<http://www.broadbandreports.com/forum/remark,14141344>

--

Steve Scherf  
steve@moonsoft.com

## SecurityFocus Bugtraq: RE: Serious flaw in Linksys wireless AP password security

On Mon, Aug 15, 2005 at 03:42:03PM -0700, Robert Thompson Jr. wrote:  
> From: "Robert Thompson Jr." <rthompson@columbiabank.com>  
> Subject: RE: Serious flaw in Linksys wireless AP password security  
> Date: Mon, 15 Aug 2005 15:42:03 -0700  
> To: Steve Scherf <bugtraq@moonsoft.com>, bugtraq@securityfocus.com  
>  
> When upgrading my WRT54GS (v 1.0) router to the 4.50.6 and 4.70.6  
> firmwares, I experienced no such authentication problems.  
>  
> If the router was set wide open, I could connect without  
authentication.  
>  
> As soon as I specified WPA-PSK on the router, in order for me to  
> connect via the NIC I absolutely had to have the WZC configured for  
> WPA-PSK (TKIP or AES accordingly) and HAD to have the correct password  
> configured as well. (And the SSID of course...)  
>  
> If the proper settings were not configured into the WZC after enabling  
> WPA-PSK, I was not able to connect to the router.  
>  
> I am certain of these details as I was trying to get the WPA2 feature  
> to work on my NIC that didn't have WPA2 certified drivers at the time.  
> I ended up trying every damned near possible configuration before  
> realizing that it was my drivers that weren't working on my NIC before  
> having to settle with just WPA until Linksys updated their drivers on  
> their website...  
>  
> Though, since we are on the subject of the WRT54GS router. The 4.50.6  
> and 4.70.6 firmwares enable the WPA2 feature. AND Linksys was kind  
> enough to finally release WPA2 certified drivers for the WPC54GS NIC's  
> (and I am assuming the WPC54G) as well. So if you haven't updated,  
> you may want to consider doing so for the increased security.  
>  
> Rob.  
>  
>  
>  
> -----Original Message-----  
> From: Steve Scherf [mailto:bugtraq@moonsoft.com]=20  
> Sent: Sunday, August 14, 2005 12:53 AM  
> To: bugtraq@securityfocus.com  
> Subject: Serious flaw in Linksys wireless AP password security  
>  
> It appears that firmware version 4.50.6 for the Linksys WRT54GS  
> (hardware version 1) wireless router allows wireless clients to  
> connect and use the network without actually authenticating. With WPA  
> Personal/TKIP authentication enabled, the unit allows both clients  
> using encryption with the correct settings and key, and clients not  
> using any encryption. It disallows clients attempting to use  
> encryption with the wrong settings and/or key.  
>  
> In other words, even if you think you've secured your wireless network  
> from unauthorized access, anyone can access it. It actually shows up  
> as having no password security on a Macstumbler scan, which is how I  
> noticed the problem.  
> I verified that anyone can access the network without needing to know  
> the key.  
>  
> I did not check security modes other than WPA/TKIP. Other modes may  
> have different behavior. Changing the "Authentication Type" setting  
> had no effect on this problem. I believe it should be set to "Shared  
> Key", but the setting used does not appear to matter.

## SecurityFocus Bugtraq: RE: Serious flaw in Linksys wireless AP password security

>  
> I only verified the problem on firmware 4.50.6. It is unknown if other  
> firmware versions exhibit the problem. However, at least one older  
> firmware does not exhibit the problem, as my router functioned  
> correctly until I updated to 4.50.6.  
>  
> The problem appears to be fixed in version 4.70.6. No explicit notice  
> of this problem or the fix appears in the release notes for version  
> 4.70.6.  
> Strangely, the "Authentication Type" must be set to "Auto" for the  
> unit to function properly. Should it be set to "Shared Key", which one  
> might expect to be the correct value, the wireless functionality  
> appears to be entirely disabled.  
>  
> It is unknown if this problem is seen with other hardware versions, or  
> with other models. I suspect it may, given the similarity between many  
> of the Linksys models and their firmware.  
>  
>  
> --  
> Steve Scherf  
> bugtraq@moonsoft.com