

[NEWS] Linksys WRT54GS WPA Personal/TKIP Authentication Flaws

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0082.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/05

To: list@securiteam.com

Date: 18 Aug 2005 17:02:54 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Linksys WRT54GS WPA Personal/TKIP Authentication Flaws

SUMMARY

Linksys WRT54GS is "Internet-sharing Router, 4-port Switch, and performance enhanced Wireless-G (802.11g) Access Point". A flaw in Linksys WRT54GS Wireless Router allows unauthorized access when WPA/TKIP authentication mode is on.

DETAILS

Vulnerable Systems:

- * Linksys WRT54GS firmware version 4.50.6

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 http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access WPA Personal/ <http://en.wikipedia.org/wiki/TKIP> 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.

Securiteam: [NEWS] Linksys WRT54GS WPA Personal/TKIP Authentication Flaws

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 the problem noticed. It was verified that anyone can access the network without needing to know the key.

No security modes other than WPA/TKIP were checked. Other modes may have different behavior. Changing the "Authentication Type" setting had no effect on this problem. Its believed it should be set to "Shared Key", but the setting used does not appear to matter.

The problem was verified only 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 router functioned correctly until 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. Its suspected it may, given the similarity between many of the Linksys models and their firmware.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bugtraq@moonsoft.com>> Steve Scherf.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.