

# [NEWS] Linksys WAP11 Password in Clear Text Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0018.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 04/14/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Apr 2003 16:50:08 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Linksys WAP11 Password in Clear Text Vulnerability

---

## SUMMARY

"The Instant Wireless Network Access Point from Linksys delivers the freedom to configure your network your way. Utilization of "state-of-the-art" wireless technology gives you the ability to set up workstations in ways you never thought possible; no cables to install means less expense and less hassle.

The Instant Wireless Access Point's high-powered antenna offers a range of operation of up to 1640 feet, providing seamless roaming throughout your wireless LAN infrastructure..."

Direct quote from LinkSys's website:

<<http://www.linksys.com/Products/product.asp?prid=157&grid=22>>

<http://www.linksys.com/Products/product.asp?prid=157&grid=22>

The admin password to the Linksys Wireless Access Point is transmitted in plaintext over the web, allowing an attacker to discover it.

## DETAILS

## Securiteam: [NEWS] Linksys WAP11 Password in Clear Text Vulnerability

Vulnerable systems:

Version 2.2 Firmware 1.1

Immune systems:

Version 2.6 Firmware 1.06

Vulnerability details:

The LinkSys Wireless Network Access Point enables users to modify the admin password via web interface.

After the user entered the new password, it is transmitted back to the base station in plaintext, thus allowing any remote user who can pick up the transmission to gain admin access to the Access Point.

PoC:

1. Open Web Browser
2. Type in Wireless Access Point IP Address in the address bar
3. Log into Access Point with Password
4. Click on Password
5. Change Password Click Apply.
6. Password is displayed in Address Bar.

### ADDITIONAL INFORMATION

The information has been provided by  
<mailto:[eric\\_b\\_gonzalez@rocketmail.com](mailto:eric_b_gonzalez@rocketmail.com)> Eric B. Gonzalez.

=====

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](mailto:list-unsubscribe@securiteam.com)

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