

# [NT] Atmel SNMP Non Public Community String DoS Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0113.html>

---

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

*Date:* 12/25/01

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

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

Date: Tue, 25 Dec 2001 22:15:51 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Atmel SNMP Non Public Community String DoS Vulnerability

---

## SUMMARY

During some tests, it was noted that the 1.3 version firmware contains a flaw that may result in a denial-of-service, preventing any new further request to be correctly handled by the device.

## DETAILS

Vulnerable systems:

Atmel Firmware 1.3

If an SNMP read request is made with a community name different than "public" (including NULL community string) or an unknown OID, it leads to a denial of service even if the answer is correct (i.e. the returned code error in the reply is ok). Any SNMP request made to the Wireless Access Point is then denied. Reset of the appliance is necessary to recover normal functioning.

Vendor status:

Linsys was contacted October 30, 2001 and answered. They say that the 1.3 firmware for the WAP11 is a somewhat dated release. The current shipping version is 1.4g.5.

Securiteam: [NT] Atmel SNMP Non Public Community String DoS Vulnerability

Workaround:

The vendor suggested the following: "for customers that have earlier versions, new code is available on our ftp site:

<<ftp://ftp.linksys.com/pub/network/wap11fw14g5.exe>>  
<ftp://ftp.linksys.com/pub/network/wap11fw14g5.exe>.

The new utility is also required to use this firmware, also available on our ftp site : <<ftp://ftp.linksys.com/pub/network/wap11sw.exe>>  
<ftp://ftp.linksys.com/pub/network/wap11sw.exe>.

These links are also published on our website at:

<<http://www.linksys.com/download/firmware.asp>>  
<http://www.linksys.com/download/firmware.asp> under the wap11 section from the drop down."

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:frederic.brouille@vigilante.com>> Frederic Brouille.

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Apache's mod\_bf Vulnerable to a Buffer Overflow and DoS"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)