

# [NEWS] D-Link DWL-1000AP can be Compromised Due to Insecure SNMP Configuration

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0111.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 08:08:56 +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.

-----

D-Link DWL-1000AP can be Compromised Due to Insecure SNMP Configuration

---

## SUMMARY

A security vulnerability in

<<http://www.dlink.com/products/wireless/dw11000ap/>> D-Link DWL-1000AP allows an attacker to gain the administrative password using a simple SNMP get command.

## DETAILS

Vulnerable systems:

DWL-1000AP Wireless Access (3.2.28 #483)

Due to the fact the DWL-1000AP uses SNMP by default; a weakness in the product allows attackers to hijack the access point. This happens even if the DWL has been enabled to use a 128-bit WEP, a non-default admin password has been set, a non-default SSID name is used, and the configuration is to disallow all MACs except for those explicitly allowed.

A MIB walk using the read-only SNMP community of 'public' (default read-only community for most devices) can allow an attacker access to the

## Securiteam: [NEWS] D-Link DWL-1000AP can be Compromised Due to Insecure SNMP Configuration

"admin password" to the access point listed in clear text in OID 1.3.6.1.4.1.937.2.1.2.2.0 as a string value.

By telling the SNMP utility to use "snowball" as the write community, it is possible to reset the value stored in that OID to any arbitrary value.

This means that anyone armed with a simple SNMP utility that can perform read and write operations, can read the private community name (which defaults to "public" with no way to change it using D-Link's configuration software), and access to the network connected to the Ethernet port of the access point. Further, an attacker could hijack the access point and either simply configure the product to allow him access to the wireless network or completely change the configuration and cause a denial of service.

The only protection currently offered by the access point against this attack is the lock-access point procedure. This is not an option in most cases since the access point may be mounted in a hard to access area, for example, in which case a simple configuration change would require physical access to the device, which may be impractical in all situations.

A more practical solution would be to give the user the ability to set both the read-only (found in OID 1.3.6.1.4.1.937.2.1.2.1.0) and write community names. This can currently be done, by using an SNMP utility to write to the read-only community OID. By changing that community, an attacker would have to sniff SNMP packets across the network or otherwise figure out the read-only community, a more difficult task than simply using the default read-only community for most SNMP devices. By giving the user the ability to control the read-only community value through the HTTP configuration, it would be a very simple task for that user to change the value during the initial setup and thus increase the security of the access point.

Vendor response:

D-Link responded with this message:

Dear Valued Customer,

In regards to your e-mail, I agree however, the dwl-1000 is intended for residential use. It does not put out enough wireless signal to cause much concern of hackers. The hacker would have to be sitting outside your house by the window.

Thank you for your technical question and feedback. If you are continuing to have problems, please contact our live support at 800-758-5489 or resubmit the problem at <http://www.dlink.com/tech/contact/>.

Thank You,  
D-Link US Technical Support  
949-790-5290

## Securiteam: [NEWS] D-Link DWL-1000AP can be Compromised Due to Insecure SNMP Configuration

This response seems to be unsatisfactory, considering how easy it would be to allow a user to change the read community name.

### Workaround:

Anyone who has a DWL-1000AP is encouraged to use an SNMP utility to change the read community stored in OID (1.3.6.1.4.1.937.2.1.2.1.0).

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[jstrine@netpanel.com](mailto:jstrine@netpanel.com)>  
Jonathan Strine.

=====

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] Webmin view\_man.cgi Security Vulnerability"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)