

[NMRC Advisory] Microsoft Windows Wireless Exposure on Laptops

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-01/msg00236.html>

- *From:* Advisories <advisories@xxxxxxxx>
 - *Date:* Sat, 14 Jan 2006 12:50:57 -0600 (CST)
-

Nomad Mobile Research Centre
A D V I S O R Y
www.nmrc.org
Simple Nomad [thegnome@xxxxxxxx]
14Jan2006

Microsoft Windows Silent Adhoc Network Advertisement

Platforms : Windows 2000/XP/2003
Application: Wireless Network Connection
(aka Microsoft Wireless Client)
Severity : High (albeit lame)

Synopsis

This advisory documents an anomaly involving Microsoft's Wireless Network Connection. If a laptop connects to an ad-hoc network it can later start beaconing the ad-hoc network's SSID as its own ad-hoc network without the laptop owner's knowledge. This can allow an attacker to attach to the laptop as a prelude to further attack.

Details

[NMRC Advisory] Microsoft Windows Wireless Exposure on Laptops

The following is a sample scenario:

- Alice has a wireless access point at home with an SSID of "linksys", which she has successfully set up and connected to with her laptop.
- Alice goes to the airport (or train station or coffee shop) and opens her laptop.
- Bob, who is sitting next to Alice, has a laptop configured with an ad-hoc network advertising an SSID of "linksys".
- Alice's laptop when started looks for the SSID of "linksys", and attaches to Bob's ad-hoc network.
- The next time Alice boots up the laptop when the Ethernet cable is not attached and there is no "linksys" SSID in range, Alice starts advertising an ad-hoc network with an SSID of "linksys".

This is basically a configuration error that spreads virus-like from laptop to laptop. In field tests, numerous ad-hoc SSIDs such as "linksys", "dlink", "tmobile", "hpsetup", and others have been documented.

The issue is compounded with a few additional caveats. Laptops with built-in wireless connectivity are usually left with the wireless active. Additionally, by default most wireless connections use DHCP to acquire an IP address. If the DHCP request fails, Microsoft has implemented RFC 3927