

[NT] Microsoft Windows Wireless Exposure on Laptops

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00054.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 17:28:06 +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>

Microsoft Windows Wireless Exposure on Laptops

SUMMARY

If a Windows based 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

Vulnerable Systems:

- * Microsoft Windows 2000 SP2 Wireless Network Connection
- * Microsoft Windows 2000 SP3 Wireless Network Connection
- * Microsoft Windows 2000 SP4 Wireless Network Connection
- * Microsoft Windows XP Home Edition Gold Wireless Network Connection
- * Microsoft Windows XP Professional Edition Gold Wireless Network Connection
- * Microsoft Windows XP Professional SP1 Wireless Network Connection
- * Microsoft Windows XP Professional SP2 Wireless Network Connection
- * Microsoft Windows 2003 Wireless Network Connection

The following is a sample scenario:

[NT] Microsoft Windows Wireless Exposure on Laptops

[NT] Microsoft Windows Wireless Exposure on Laptops

- 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](http://www.faqs.org/rfcs/rfc3927.html) to provide an IP address via [APIPA](http://en.wikipedia.org/wiki/APIPA) (Automated Private IP Address) in the 169.254.0.0/16 range. This is known as a Link-Local address, and by default Link-Local is turned on on all Windows platforms on all interfaces, including wireless interfaces. Details of Microsoft's Link-Local implementation is in RFC 3927, appendix A.4 (Microsoft is a co-author of RFC 3927).

Essentially this assigns the advertising ad-hoc network an IP address. On Windows 2000 and Windows XP SP0 and SP1, this all happens in the background without the user's knowledge — on Windows XP SP2, the user is notified it has "attached" to an ad-hoc network, when in fact it has simply started advertising the ad-hoc network and the Link-Local address has been assigned. An attacker can attach to the ad-hoc SSID and either manually assign an IP address in the 169.254 class B or simply DHCP and await a time-out that assigns the attacker's laptop an IP address via a Link-Local configuration. After passively sniffing and awaiting the usual NetBIOS traffic and/or by running a ping sweep, the victim's IP address can be discovered. The attacker can then perform the various probes and attacks to gain access to the system.

If the attacker is impatient in waiting for determining the IP address of the victim computer, the attacker can attach to the advertising SSID and offer up a DHCP server. Windows systems running Link-Local addresses periodically probe for a DHCP address, so the victim will eventually get the DHCP address and switch to the new address supplied by the DHCP as opposed to continue using the APIPA number. By tracking what IP addresses are being served by the DHCP server, the attacker can spend more time on an attack and less time solving the connectivity issue.

There is a warning about using Link-Local with wireless LANs due to the

[NT] Microsoft Windows Wireless Exposure on Laptops

lack of physical security in RFC 3927 section 5 paragraph 3, but unfortunately Microsoft failed to properly heed this warning in spite of co-authoring the RFC.

In field tests, it became apparent that if the laptop user fired up their laptop in the airport terminal and was advertising an ad-hoc network, when the same laptop user fired up their laptop during the flight, they would in fact be advertising the ad-hoc network during flight. This has a couple of ramifications.

The first is that if wireless laptops with the wireless adapter enabled were capable of interfering with the navigational systems as claimed by the airlines then we would be having numerous in-flight incidents due to the high proliferation of wifi-enabled laptops used by business people on flights. The second ramification is that users sitting on a plane at 35,000 feet are not going to be suspecting a network attack against the laptop in the lap, and so any odd "side effects" from probe and attack attempts (service crashing, blue screen or a restart) will be dismissed as a local system anomaly and not an attack, allowing the attacker to be a little more aggressive.

Here is collected data from 4 domestic flights within the U.S. conducted during September and October 2005. The data was collected using <http://www.netstumbler.com> NetStumbler, <http://www.insecure.org/nmap> Nmap, and <http://www.metasploit.com> Metasploit Framework from a laptop running Windows XP:

Aircraft Laptops* Ad-hoc Nets** Live Targets Vulnerable***

MD80 8 2 3

1

MD80 12 5 5

4

757 22 1 3

3

MD80 14 4 4

3

* Number of laptops out and running at approximately the halfway point of the flight.

** In some cases, an ad-hoc network would form and other laptops would attach to it instead of advertising their own ad-hoc network.

*** A system was classified as vulnerable if it could be remotely compromised or it was open enough to allow files to be copied to or from the hard drive. Vulnerabilities included

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0059>

CVE-2005-0059 (<http://www.securiteam.com/windowsntfocus/5BP0B0UFGY.html> MS05-017),

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1983>

CVE-2005-1983 (<http://www.securiteam.com/windowsntfocus/5YP0E00GKW.html>)

[NT] Microsoft Windows Wireless Exposure on Laptops

MS05-039), open shares, and NULL access.

It should also be noted that while visiting Charlotte, NC (whose airport at the time had no commercial wireless offering like TMobile or anything else) — walking the terminal during massive eastcoast rain delays with most flights delayed by a couple of hours — I counted no less than 62 ad-hoc devices. The novelty of collecting data during flight was the focus of the table above, but a conservative estimate would put have of those ad-hoc devices at risk.

Vendor Status:

Microsoft was contacted on October 13, 2005. After numerous exchanges of emails and a conference call, Microsoft was able to reproduce and isolate the issue within their software. As there are multiple and easy-to-implement workarounds for the issue, Microsoft has scheduled to include the fix in the next service packs.

Workaround:

Until Microsoft releases Service Packs for the affected platforms, use one of the following three workarounds:

Workaround #1:

Disable wireless when not in use.

Workaround #2:

Use an alternate Wireless Client Manager, (e.g. for an integrated Intel Wifi connector, use Intel PROSet/Wireless) as all others tested do not seem to have the problem (this testing was not all-inclusive).

Workaround #3 (recommended):

1. Click on the Wireless option in the System Tray and open the Wireless Network Connection window.
2. Click on "Change advanced settings".
3. In the Wireless Network Connection Properties window, click on the Wireless Networks tab.
4. Click on the Advanced button.
5. Click on "Access point (infrastructure) networks only"

This workaround prevents you from connecting to any ad-hoc network in the first place.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@xxxxxxxx>> Simple Nomad.

Additional testing tools can be found at:

<<http://www.theta44.org/karma/index.html>>

<http://www.theta44.org/karma/index.html>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.



- Prev by Date: [*\[TOOL\] Dnsgrep – DNS Enumeration Tool*](#)
- Next by Date: [*\[NEWS\] ZyXel P2000W VoIP Information Disclosure and DoS*](#)
- Previous by thread: [*\[TOOL\] Dnsgrep – DNS Enumeration Tool*](#)
- Next by thread: [*\[NEWS\] ZyXel P2000W VoIP Information Disclosure and DoS*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)