

# [TOOL] WaveLock, WLAN Policy Enforcement

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0038.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 02/16/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 16 Feb 2003 23:10:26 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

WaveLock, WLAN Policy Enforcement

---

## DETAILS

Windows 2000 and Windows XP come with drivers for several wireless LAN ("WLAN") adapters; installation requires only insertion of one of those adapters. Administrative privileges are not required, as no new drivers must be registered with the operating system. WaveLock assists in enforcing security policies by blocking access to these adapters, making it harder to circumvent firewalls, filters, proxies, and other required safeguards.

To install WaveLock, download and uncompress wavelock.zip. Execute the resulting wavelock.msi file (a Windows Installer setup), which installs wavelock.sys. Reboot to load and activate WaveLock.

A list of the wireless network adapters supported out-of-the-box on Windows 2000 and Windows XP can be found below. Note that WaveLock cannot know about and will therefore not block additional drivers installed by administrators.

## The Risk

In corporate environments, the network infrastructure is usually carefully secured against attacks from the outside, and abuse from the inside. Yet all these precautions can be worked around if a second network, parallel

to the corporate one, can be created. Nothing makes this easier than a wireless network adapter: Notebook computers now often have WLAN adapters built-in; and those that do not can have a PCcard (formerly PCMCIA) adapter installed in literally a flick of the wrist.

These adapters, so far, all lack in security due to deficient WLAN standards -- programs to search for and hack into wireless networks are freely available from a number of web and FTP sites. Especially in networks with security-sensitive information, broadcasting that information to anyone with a notebook, one of those hacking programs, and a few minutes of time is probably undesirable.

In addition to the risk of disclosing sensitive data, WLAN adapters also open computers to the introduction of malicious software, effectively making an end-run around the expensive and carefully maintained firewall that is supposed to prevent just that malicious software from reaching the network.

Like all hardware devices, WLAN adapters require drivers to work. A driver is a program module that "knows" how to communicate with the device; drivers are loaded by Windows upon booting the system or activating a device.

Such drivers can normally only be installed by administrators, which would prevent the installation of WLAN adapters. Unfortunately, that restriction does not apply to the WLAN drivers that are included with Windows 2000 and Windows XP: Anyone can insert one of the WLAN adapters supported by out-of-the-box Windows and have it working in seconds, without being an administrator.

#### The Solution

WaveLock, when installed, is loaded by Windows before any WLAN adapter drivers. From then on, it examines every device for which Windows tries to load a driver, as well as the drivers themselves.

If a driver (and device) being loaded by Windows are on the list of WLAN adapters that can be installed without requiring administrative privileges, WaveLock will not allow the driver to load, rendering the wireless network adapter inoperative.

We have created a list of the WLAN adapters that Windows may load without an administrator's permission; this is also the definitive list of devices whose use will be prevented by WaveLock. You can find that list in the Readme file that is part of the WaveLock software, and we have duplicated it below for your convenience (Windows 2000, Windows XP).

With no configuration beyond the installation of the WaveLock software itself, and with no negative consequences for any other part of the system, WaveLock is among the easiest solutions that security threats ever had.

ADDITIONAL INFORMATION

The tool can be downloaded from:

<[http://securewave.com/products/free\\_utilities/wavelock.html](http://securewave.com/products/free_utilities/wavelock.html)>  
[http://securewave.com/products/free\\_utilities/wavelock.html](http://securewave.com/products/free_utilities/wavelock.html)

The information has been provided by <mailto:[marco@securewave.com](mailto:marco@securewave.com)> Marco PERETTI.

=====

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.