

# [NT] WinPcap NPF.SYS bpf\_filter\_init Arbitrary Array Indexing Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00027.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 14 Nov 2007 19:33:03 +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>

-----

WinPcap NPF.SYS bpf\_filter\_init Arbitrary Array Indexing Vulnerability

---

## SUMMARY

<<http://www.winpcap.org/>> WinPcap is "a software package that facilitates real-time link-level network access for Windows-based operating systems. A wide range of open-source projects, including Wireshark, use it". Local exploitation of an invalid array indexing vulnerability in the NPF.SYS device driver of WinPcap allows attackers to execute arbitrary code in kernel context.

## DETAILS

Vulnerable Systems:

- \* WinPcap version 4.0.1 included in Wireshark version 0.99.6a
- \* NPF.SYS version 4.0.0.901

Immune Systems:

- \* WinPcap version 4.0.2

The problem specifically exists within the bpf\_filter\_init function. In several places throughout this function, values supplied from a potential attacker are used as array indexes without proper bounds checking. By

## [NT] WinPcap NPF.SYS bpf\_filter\_init Arbitrary Array Indexing Vulnerability

making IOCTL requests with specially chosen values, attackers are able to corrupt the stack, or pool memory, within the kernel.

### Analysis:

Exploitation allows attackers to execute arbitrary code in kernel context.

The vulnerable device driver is loaded when WinPcap is initialized. This driver can be set to load on start-up depending on a choice made at installation time. However, this is not the default setting.

Normally, the device driver is not loaded until an administrator utilizes a WinPcap dependent application. Once they do, it will become accessible to normal users as well. When a program using this driver exits, it is not unloaded. Attackers will continue to have access until the driver is manually unloaded.

If the option to allow normal user access was chosen at installation time, attackers will always have access to this device driver. Consequently, a local attacker without administrator privileges would have access to sniff, as well as exploit this vulnerability.

### Vendor response:

The WinPcap Team has addressed this vulnerability by releasing version 4.0.2 of the WinPcap software. For more information, see the following URL: <<http://www.winpcap.org/misc/changelog.htm>>  
<http://www.winpcap.org/misc/changelog.htm>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5756>>  
CVE-2007-5756

### Disclosure timeline:

10/30/2007 – Initial vendor notification  
10/30/2007 – Initial vendor response  
11/12/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=625>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=625>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[NT] WinPcap NPF.SYS bpf\_filter\_init Arbitrary Array Indexing Vulnerability

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

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

=====  
=====

**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.