

# [NEWS] More Information Regarding Etherleak

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0040.html>

---

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

*Date:* 01/13/03

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

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

Date: 13 Jan 2003 11:50:30 +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)

-----

More Information Regarding Etherleak

---

## SUMMARY

The following advisory will try to shed some additional light on the issue we illustrated in:

<<http://www.securiteam.com/securitynews/5BP01208UO.html>> Etherleak: Ethernet Frame Padding Information Leakage.

## DETAILS

Who is vulnerable?

Josh Anderson and Ofir Arkin tested several Ethernet cards and device drivers.

They have found several device drivers which are vulnerable but they never attempted to find them all. It is simply because there are too many.

Therefore they have contacted CERT more than 6 months ago and sent them the Etherleak paper and asked them to contact OS manufactures, Network device manufactures, Chipset manufactures, motherboard manufactures and other manufactures and vendors who might need to check their device driver's implementations.

In their tests they have experienced this bug under 4 different operating systems:

## Securiteam: [NEWS] More Information Regarding Etherleak

- Linux
- NetBSD
- FreeBSD
- Microsoft Windows

One of the Ethernet cards and device drivers they have tested was a Compaq PCMCIA Ethernet card under Windows 2000 (with the latest SP at the time) which demonstrated the vulnerability (among other Ethernet cards which have demonstrated the vulnerability under Microsoft Windows 2000).

It is clear to us that device drivers under the various Microsoft operating systems are vulnerable.

Microsoft's statement to CERT:

"Microsoft does not ship any drivers that contain the vulnerability. However, they have found samples in their documentation that, when compiled without alteration, could yield a driver that could contain this issue. They have made corrections to the samples in their documentation, and will include tests for this issue in their certification process."

If you read the statement carefully you can understand that there are OTHER manufactures which have built device drivers for their networking equipment that are based on Microsoft's documentation and therefore MIGHT BE VULNERABLE.

Microsoft does not make vulnerable device drivers BUT Microsoft's sample code was vulnerable and therefore Microsoft has added a test to the device driver's certification test which will test for the bug. The situation is that CURRENT Microsoft certified device drivers MIGHT BE VULNERABLE.

Different vendors were contacted by CERT more than 6 months ago and had an enormous amount of time to fix this issue before it went public. The authors did not receive a list of vendors who were notified by CERT. The authors were aware that Microsoft was one of the vendors who were contacted and notified regarding this vulnerability.

The examples in the paper are given from the Linux operating system because it helps to illustrate the problem.

Why this vulnerability is so wide spread?

Some networking gear manufactures choose to purchase (in some cases) chipsets from a chipset manufacture rather than developing their own (or using their own). Therefore you might find networking cards from one vendor with chipsets of another chipset manufacture (for example some low-end SMC cards are using RealTek chipsets). Some other manufactures are embedding networking cards with their products (such as motherboards with LAN). To minimize the cost, sometimes, low-end chipsets, which many of whom have vulnerable device drivers on different operating system, are used (some vulnerable device drivers are even shipped with some cards...).

## Securiteam: [NEWS] More Information Regarding Etherleak

How can you test your network card and device driver?

You need to send packets which are less than 46 data bytes long (the minimum packet size) to examine if you experience this vulnerability with your Ethernet card and device driver. Any packet less than 46 data bytes long would do the trick but they have found the following examples helpful:

– An ICMP Echo request packet with 1 data byte in its payload (total of 29 bytes). The rest – 17 data bytes will be filled with information (you can see for yourself in the paper they have written what kind of information it will be) if your Ethernet card's device driver is vulnerable.

– You can also use Raw Packets and then have 28 data bytes as room for padded data.

Why is this better than a sniffer? or Why is this bug important?

First Example:

You can extract information that you will never be able to see on a switched environment.

A Second Example:

In some cases you will be able to extract information directly from a Router on your LAN (try this with a Linux or a NetBSD machine acting as a router with vulnerable Ethernet cards (and their device drivers) and see for yourself how easily information is being gleaned) or from another networking equipment on your LAN.

A Third Example:

Another example might be a corporate network (just think about the scenario of a nice flat switched network).

There are special instances where the padded information might cross layer 2 boundaries, but they are very unique in nature and depend on many factors.

Combining the information is not a trivial task for script kiddies. If you are experienced with networking and seen and analyzed network traffic in the past you will be able to understand what are the portions of information you are absorbing (see the examples in the paper).

In their tests they were able to extract pop3 passwords, other clear text passwords, cookies, and other interesting pieces of information.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:ofir@sys-security.com>> Ofir Arkin.

=====

Securiteam: [NEWS] More Information Regarding Etherleak

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.