

# [NT] Internet Explorer Clipboard Stealing Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0079.html>

---

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

*Date:* 01/16/02

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

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

Date: Wed, 16 Jan 2002 07:43:52 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

## Internet Explorer Clipboard Stealing Vulnerability

---

### SUMMARY

Since Microsoft Internet Explorer version 5.0, there has been a way to read and set the users clipboard text from script, by default, and with no prompting. This can be handy for web-based applications to do so, but can be used in a malicious way to steal the clipboard contents.

### DETAILS

It is easily possible to monitor the contents of the clipboard, and send it to a remote server-side script for processing. The remote script could then save the clipboard text in a database, or e-mail it to the evil overlord script creator. By itself this doesn't cause much harm, but users can often copy sensitive information to the clipboard -- e-mails, addresses, passwords, pictures -- just about anything, which could then fall into the wrong hands.

The problem lies in the clipboardData object[1], and the getData method[2]. By simply using a setInterval [3], a script can check for a change in the contents of the clipboard, and forward it either using a hidden form, or the XMLHTTP [4] ActiveX object.

## Securiteam: [NT] Internet Explorer Clipboard Stealing Vulnerability

Exploit:

You can view a sample exploit at:

<<http://tom.vpwsys.co.uk/clipboard/exploit.html>>

<http://tom.vpwsys.co.uk/clipboard/exploit.html> (IE5.0+, with default security rules). This does no harm to your computer, and does not send any information to the author. More information about Data Transfer can be found in the MSDN article, about DHTML Data Transfer[5].

In the most evil of situations, this could be used for an almost un-closeable clipboard monitor (see the 2nd example [6]). It could be launched from a HTML e-mail within Outlook or Outlook Express (if the security zone is set to "Internet", and the internet zone settings are set to default – basically the default settings of pre-OE6), and maybe be used in conjunction with an e-mail worm to send itself on.

User solution:

You can edit this via Tools > Internet Options > Security > Select a security zone > Custom Level > Scripting > Allow paste operations via script. You can set this to Enable (the default for the internet zone), Disable (default for restricted sites) or Prompt. It is recommend you set it to prompt – scripts can still have clipboard access, but only when you say so.

### ADDITIONAL INFORMATION

Handy links:

[1] clipboardData object –

<<http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/clipboarddata.asp>>

<http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/clipboarddata.asp>

[2] getData method –

<<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/getdata.asp>>

<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/getdata.asp>

[3] setInterval method –

<<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/setinterval.asp>>

<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/setinterval.asp>

[4] XMLHttpRequest object –

<[http://msdn.microsoft.com/library/en-us/xmlsdk/htm/xml\\_obj\\_ixmlhttprequest\\_8bp0.asp](http://msdn.microsoft.com/library/en-us/xmlsdk/htm/xml_obj_ixmlhttprequest_8bp0.asp)>

[http://msdn.microsoft.com/library/en-us/xmlsdk/htm/xml\\_obj\\_ixmlhttprequest\\_8bp0.asp](http://msdn.microsoft.com/library/en-us/xmlsdk/htm/xml_obj_ixmlhttprequest_8bp0.asp)

[5] About DHTML Data Transfer –

<<http://msdn.microsoft.com/workshop/author/datatransfer/overview.asp>>

<http://msdn.microsoft.com/workshop/author/datatransfer/overview.asp>

[6] Exploit examples – <<http://tom.vpwsys.co.uk/clipboard/exploit.html>>

<http://tom.vpwsys.co.uk/clipboard/exploit.html>

The information has been provided by <<mailto:tom@vpwsys.co.uk>> Tom Gilder and <<mailto:takagi.hiromitsu@aist.go.jp>> TAKAGI, Hiromitsu.

=====

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:

[NT] Internet Explorer Clipboard Stealing Vulnerability

Securiteam: [NT] Internet Explorer Clipboard Stealing Vulnerability

[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.

---

- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[NT] MSIE May Download and Run Programs Automatically (Details and Exploit)"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)