

# [NT] MSIE May Download and Run Programs Automatically (Details and Exploit)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0078.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 07:39:12 +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.

-----

MSIE May Download and Run Programs Automatically (Details and Exploit)

---

## SUMMARY

As we reported in our previous article: File Extensions Spoofable in MSIE Download Dialog (and Also Opera), a security vulnerability would allow a malicious site to casue a web user to unwillingly execute files because they are made to think their file extension is another than that being displayed.

## DETAILS

The flaw allows a malicious web site to make Internet Explorer download and run programs when a user is visiting the web site or reading an HTML mail message. By exploiting it, any download and Security Warning dialogs can be circumvented. The program starts without further user interaction.

The trick is simply to use a null byte in the filename. A malicious web server can set a filename like "README.TXT%00PROG.EXE" via the Content-disposition HTTP header. If this kind of filename is set for an attachment, IE will display just "README.TXT" in the download dialog (unless patched). Apparently, "%00" gets decoded and some of the string handling functions believes the filename strings ends there. When opening the file (if the user chooses to "Open" it) though, the whole filename is

## Securiteam: [NT] MSIE May Download and Run Programs Automatically (Details and Exploit)

used and the program is run.

If the keyword "inline" is used with the Content-disposition header instead of "attachment" and the MIME type is chosen right, then the browser downloads and runs the program without any download dialogs or warnings. The MIME type of the file can be set via the Content-type HTTP header. The MIME types causing the file to be automatically run seem to vary in different IE versions. With IE6, e.g. "text/css" can be used to produce the effect. With IE5, e.g. "audio/midi" can be used instead.

The "file name spoofing" and "automatic running of programs" issues are in effect the same null byte vulnerability. The MIME type determines whether the program gets started automatically or the download dialog is used.

Demonstration:

If you want to check if your browser is vulnerable, you can do it on this web page:

<<http://www.solutions.fi/iebug2>> <http://www.solutions.fi/iebug2>

After clicking the link there, a vulnerable IE will download a small program and run it. The program will run in a DOS window and print a message. If this happens, you should patch your browser. The patch has been available since 13 December 2001 at Microsoft's site:

<<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>>  
<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>

A non-vulnerable IE will show a download dialog with a filename ending with ".EXE".

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:jouko@solutions.fi>> Jouko Pynnonen.

=====

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.

---

• *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] PHP 4.x Session Spoofing"

Securiteam: [NT] MSIE May Download and Run Programs Automatically (Details and Exploit)

- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]