

Securiteam: [NT] Microsoft Internet Explorer Still Download and Execute any Program Automatically

[NT] Microsoft Internet Explorer Still Download and Execute any Program Automatically

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0071.html>

From: support@securiteam.com

Date: 05/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 18 May 2002 22:25:07 +0200 (CEST)

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.

Microsoft Internet Explorer Still Download and Execute any Program Automatically

SUMMARY

Microsoft Internet Explorer contains a vulnerability that allows for downloading of a file and its automatic execution under several circumstances without the knowledge of the user. If a malicious webmaster creates a website containing malicious contents that can exploit this problem, and if the user has access to these contents using Internet Explorer under specific environments, then arbitrary programs specified by the administrator will be automatically downloaded and executed on the user's system.

DETAILS

Vulnerable systems:

* Windows NT 4.0 Workstation + SP6a + IE 6 + all available fixes

[Japanese version]

* Windows NT 4.0 Workstation + SP6a + Windows Media Player 6.4 + IE 6 +

all available fixes [Japanese version]

* Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 6.4 + IE

6 + all available fixes [Japanese version]

* Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 6.4 + IE

Securiteam: [NT] Microsoft Internet Explorer Still Download and Execute any Program Automatically

5.01 SP2 + all available fixes [Japanese version]

* Windows 98 + Windows 98 System Update + Windows Media Player 6.4 + IE 6
+ all available fixes [Japanese version]

* Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 7.1 + IE
6 + Office 2000 SR-1 + all available fixes [Japanese version]

Note: Windows Media Player 6.4 is installed by default on Windows 2000 and Windows 98.

A vulnerability exists in Microsoft Internet Explorer that could lead to automatic downloading and execution of a file under several environments. This can be achieved when a user views contents including the following header in HTTP responses:

```
Content-Type: audio/x-ms-wma
Content-Disposition: inline; filename="foo.exe"
```

It is important to note that the above-mentioned description is just an example and that this vulnerability has been confirmed exploitable using other Content-Type: headers, such as Content-Type: audio/midi.

Solution:

This problem can be eliminated by applying a patch based on the information provided by Microsoft Security Bulletin

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-023.asp>>
MS02-023

ADDITIONAL INFORMATION

The information has been provided by <<mailto:y.arai@lac.co.jp>> Yuu Arai (LAC).

=====
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

In order to subscribe to the mailing list, simply forward this email to: 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: "[NEWS] WolfMail Allows Relaying of SPAM"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)