

[NEWS] Macromedia Flash Plugin Can Read Local Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0030.html>

From: support@securiteam.com

Date: 08/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 10 Aug 2002 22:32:45 +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.

Macromedia Flash Plugin Can Read Local Files

SUMMARY

Macromedia Flash Player is the leading rich client for Internet content and applications across the broadest range of platforms and devices.

According to Macromedia, more than 90% of web users are able to view Macromedia Flash content. Macromedia Flash Player is available for all major browsers on Windows, Mac OS, and Linux as well as on device platforms such as Pocket PC and Nokia Communicator. There is a bug in Macromedia Flash Player that allows reading and sending of local files.

This can be achieved in three ways:

1. Force a http redirect to a local file
2. Place a `<base href="file:///C:/">` in the document then use a relative URL
3. Embed the flash object in a web archive (mht file) and make it seem as though it has been saved from a location on the user's hard drive, then use a relative URL.

DETAILS

Systems affected :

The vulnerability has been confirmed to work on Macromedia Flash Player 6

Securiteam: [NEWS] Macromedia Flash Plugin Can Read Local Files

under Internet Explorer 6.

Immune systems:

* Macromedia Flash version 6.0.47.0

Example :

Demonstrations of the issues described are available at:

1. Redirect issue – <<http://kuperus.xs4all.nl/flash.htm>>

<http://kuperus.xs4all.nl/flash.htm>

2. Base tag – <<http://www.xs4all.nl/~jkuperus/flash.htm>>

<http://www.xs4all.nl/~jkuperus/flash.htm>

3. MHT File embedding – <<http://www.xs4all.nl/~jkuperus/flash.mht>>

<http://www.xs4all.nl/~jkuperus/flash.mht>

All of the above examples will read and displays the contents of c:\jelmer.txt. The examples use the Macromedia Flash XML object, first introduced in Macromedia Flash Player 5 to read the local files.

There may be other ways to achieve the same effect.

Vendor status:

Macromedia was notified on July 12 2002. The latest build fixes the problem.

Workaround:

Update to the latest player (6,0,47,0). It should be available at:

<<http://www.macromedia.com/go/getflashplayer/>>

<http://www.macromedia.com/go/getflashplayer/>

ADDITIONAL INFORMATION

References:

<<http://www.netmag.co.uk/ie5/save-page.htm>>

<http://www.netmag.co.uk/ie5/save-page.htm>

<<http://www.wdvl.com/Authoring/HTML/Head/base.html>>

<http://www.wdvl.com/Authoring/HTML/Head/base.html>

<<http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.3>>

<http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.3>

<http://www.macromedia.com/support/flash/action_scripts/objects/xml_object.html>

http://www.macromedia.com/support/flash/action_scripts/objects/xml_object.html

<http://www.macromedia.com/software/player_census/flashplayer/version_penetration.html>

http://www.macromedia.com/software/player_census/flashplayer/version_penetration.html

Securiteam: [NEWS] Macromedia Flash Plugin Can Read Local Files

The information has been provided by <mailto:jelmer@kuperus.xs4all.nl>
Jelmer.

=====

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: "[NT] Cross-Site Scripting Issues in Falcon Web Server"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)