

[NT] Microsoft Internet Explorer Multiple Vulnerabilities (Content-Disposition, codebase)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/15/05

To: list@securiteam.com

Date: 15 Feb 2005 14:08:02 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Microsoft Internet Explorer Multiple Vulnerabilities (Content-Disposition, codebase)

SUMMARY

Secunia Research has discovered multiple vulnerabilities in Microsoft Internet Explorer, which can be exploited by malicious people to disclose sensitive information, bypass certain security restrictions and compromise a user's system.

DETAILS

Vulnerable Systems:

- * Microsoft Internet Explorer 5.01
- * Microsoft Internet Explorer 5.5
- * Windows 2000 with Internet Explorer 6
- * Windows XP SP1 with Internet Explorer 6
- * Windows XP SP2 with Internet Explorer 6

Content-Disposition Vulnerability:

The vulnerability of "Content-Disposition" is caused due to insufficient validation of drag and drop events from the "Internet" zone to local resources. Specifically when a valid image contains script code. This can

Securiteam: [NT] Microsoft Internet Explorer Multiple Vulnerabilities (Content-Disposition, codebase)

be exploited by a malicious websites to plant many different types of files on a user's system via a specially crafted "Content-Disposition" HTTP header where a dot is appended in the filename.

Example:

"Content-Disposition: attachment; filename=malicious.bat."

Temporary Internet Files:

Due to an error in the handling of websites inside the "Temporary Internet Files" folder, the problem could be exploited to cause a site to be loaded in context of the "Temporary Internet Files" folder when a user clicks on a link.

Further exploitation involves gaining knowledge of a user's user-name and retrieving documents found inside the "Temporary Internet Files" folder.

Codebase Vulnerability:

A parsing error in the "codebase" attribute of the "object" tag allows attackers to cause the execution of local files with any file extension from the "Local Computer Zone". This is done by appending an "?.exe" to the end of the filename.

NOTE: A combination of the vulnerabilities can be exploited to execute arbitrary code on Microsoft Internet Explorer running Windows 2000 and Windows XP SP1, in combination with a third-party software that stores malicious files in a predictable location.

Solution:

See solution provided by Microsoft at:

<<http://www.microsoft.com/technet/security/bulletin/ms05-014.msp>>

MS05-014.

ADDITIONAL INFORMATION

The original article can be found at:

<http://secunia.com/secunia_research/2004-8/advisory/>

http://secunia.com/secunia_research/2004-8/advisory/

The information has been provided by <<mailto:as@secunia.com>> Andreas Sandblad.

=====

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.