

[NT] Internet Explorer Object Type Buffer Overflow in Double-Byte Character Set Environment

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0058.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/21/03

To: list@securiteam.com

Date: 21 Aug 2003 09:35:40 +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>

Internet Explorer Object Type Buffer Overflow in Double-Byte Character Set Environment

SUMMARY

Microsoft Internet Explorer is vulnerable to a buffer overflow under the double-byte character set environment.

DETAILS

Vulnerable systems:

- * Internet Explorer 6 Service Pack 1 Japanese Edition

A buffer overflow occurs in Microsoft Internet Explorer when HTML files with an unusually long string including double-byte character sets in the Type property of the Object tag are processed.

In order to trigger this vulnerability, malicious website administrators could induce Internet Explorer users to view a specially crafted web site and consequently execute arbitrary code with the users' privileges.

This problem differs from the issue described in MS03-020 in that it affects only specific language versions, including Japanese. Arbitrary

Securiteam: [NT] Internet Explorer Object Type Buffer Overflow in Double-Byte Character Set Environment

codes could be successfully executed on Internet Explorer 6 SP1 Japanese in a testing environment.

Solution:

Apply an appropriate patch available at:

Microsoft Security Bulletin MS03-032:

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

Microsoft Security Bulletin MS03-032(Japanese site):

<http://www.microsoft.com/japan/technet/security/bulletin/MS03-032.asp>

<http://www.microsoft.com/japan/technet/security/bulletin/MS03-032.asp>

ADDITIONAL INFORMATION

The original advisory can be found at the following URL:

http://www.lac.co.jp/security/english/snsadv_e/68_e.html

http://www.lac.co.jp/security/english/snsadv_e/68_e.html

The information has been provided by <mailto:y.arai@lac.co.jp> Yuu Arai and <mailto:snsadv@lac.co.jp> SecureNet Service(SNS) Spiffy Reviews.

=====

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.