

# [NT] The Return of the Content-Disposition Vulnerability in IE

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0057.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 08/21/03

To: list@securiteam.com

Date: 21 Aug 2003 09:27:42 +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>

-----

The Return of the Content-Disposition Vulnerability in IE

---

## SUMMARY

Microsoft Internet Explorer is prone to a vulnerability that can, under several conditions, result in the automatic download and parse of a specific tag included with HTML files in the My Computer zone without the knowledge of the user.

## DETAILS

Vulnerable systems:

- \* Internet Explorer 6 Service Pack 1 Japanese Edition

If specific MIME type is specified in the Content-Type header of an HTTP response and if a special string is defined in the Content-Disposition header, this string can be automatically downloaded and opened within the Temporary Internet Files (TIF) under several conditions in Microsoft Internet Explorer. A malicious website administrator can induce a user to view a specially crafted web site to cause the script to be automatically executed upon viewing the malicious contents. Execution of the script can then, disclose the path to the TIF directory to the attacker.

## Securiteam: [NT] The Return of the Content–Disposition Vulnerability in IE

Additionally, if this vulnerability is exploited through a specific string in the Content–Disposition header, the OBJECT tag can be parsed in the "My Computer" zone. However, if the user has access to the malicious Web site, the attacker will be able to execute programs on the computer with the user's privileges.

### 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/67\\_e.html](http://www.lac.co.jp/security/english/snsadv_e/67_e.html)>  
[http://www.lac.co.jp/security/english/snsadv\\_e/67\\_e.html](http://www.lac.co.jp/security/english/snsadv_e/67_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.