

# [NT] Cumulative Security Update for Internet Explorer (MS03-048)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0050.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 11/12/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 12 Nov 2003 20:38:56 +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>

-----

Cumulative Security Update for Internet Explorer (MS03-048)

---

## SUMMARY

This is a cumulative update that includes the functionality of all the previously-released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0. Additionally, it eliminates the following five newly-discovered vulnerabilities:

- \* Three vulnerabilities that involve the cross-domain security model of Internet Explorer, which keeps windows of different domains from sharing information. These vulnerabilities could result in the execution of script in the My Computer zone. To exploit one of these vulnerabilities, an attacker would have to host a malicious Web site that contains a Web page that is designed to exploit the particular vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e-mail message that designed to exploit one of these vulnerabilities and persuade the user to view the HTML e-mail message. After the user has visited the malicious Web site or viewed the malicious HTML e-mail message an attacker who exploited one of these vulnerabilities could access information from other Web sites, access files on a user's system, and run arbitrary code on a user's system. This code would run in the security context of the currently logged on user.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS03-048)

\* A vulnerability that involves the way that zone information is passed to an XML object within Internet Explorer. This vulnerability could allow an attacker to read local files on a user's system. To exploit this vulnerability, an attacker would have to host a malicious Web site that contains a Web page that is designed to exploit the particular vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e-mail message that is designed to exploit this vulnerability and persuade the user to view the HTML e-mail message. After the user visits the malicious Web site or views the malicious HTML e-mail message, the user would then be prompted to download an HTML file. If the user accepts the download of this HTML file, an attacker could read local files that are in a known location on the user's system.

\* A vulnerability that involves performing a drag-and-drop operation during dynamic HTML (DHTML) events in Internet Explorer. This vulnerability could allow a file to be saved in a target location on the user's system if the user clicks a link. No dialog box would request that the user approve this download. To exploit one of these vulnerabilities, an attacker would have to host a malicious Web site that contains a Web page that has a specially-crafted link. The attacker would then have to persuade a user to click that link. The attacker could also create an HTML e-mail message that has a specially-crafted link, and then persuade the user to view the HTML e-mail message and then click the malicious link. If the user clicked this link, code of the attacker's choice could be saved on the user's computer in a targeted location.

As with the previous Internet Explorer cumulative updates that were released with bulletins MS03-004, MS03-015, MS03-020, MS03-032, and MS03-040, this cumulative update causes the window.showHelp() control to no longer work if you have not applied the HTML Help update. If you have installed the updated HTML Help control from Knowledge Base article 811630, you will still be able to use HTML Help functionality after you apply this update.

### DETAILS

#### Affected Components:

- \* Internet Explorer 6 Service Pack 1:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=9D8543E9-0E2B-46C9-B6C6-12DE03860465&disp>

Download the update

- \* Internet Explorer 6 Service Pack 1 (64-Bit Edition):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=35F99CF5-3629-4E0E-BF60-24845D2D20C9&disp>

Download the update

- \* Internet Explorer 6 Service Pack 1 for Windows Server 2003:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=35F99CF5-3629-4E0E-BF60-24845D2D20C9&disp>

Download the update

- \* Internet Explorer 6 Service Pack 1 for Windows Server 2003 (64-Bit Edition):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=8BEFA1EC-0C48-4B65-989D-58B0CE1E6F95&disp>

Download the update

- \* Internet Explorer 6:

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS03-048)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4C4D22F0-FBF7-4EA6-9CC2-27D104D4198E&dis>

Download the update

\* Internet Explorer 5.5 Service Pack 2:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E438AFD4-DF70-448C-8925-1075C8BE6C5E&dis>

Download the update

\* Internet Explorer 5.01 Service Pack 4:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C15E2DB3-14E2-43A4-A1A1-676374B66517&dis>

Download the update

\* Internet Explorer 5.01 Service Pack 3:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C15E2DB3-14E2-43A4-A1A1-676374B66517&dis>

Download the update

\* Internet Explorer 5.01 Service Pack 2:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C15E2DB3-14E2-43A4-A1A1-676374B66517&dis>

Download the update

Mitigating factors:

There are three common mitigating factors across all the vulnerabilities:

\* By default, Internet Explorer on Windows Server 2003 runs in Enhanced Security Configuration. This default configuration of Internet Explorer blocks automatic exploitation of this attack. If Internet Explorer Enhanced Security Configuration has been disabled, the protections that are put in place that prevent these vulnerabilities from being automatically exploited would be removed.

\* In the Web-based attack scenario, the attacker would have to host a Web site that contains a Web page that is used to exploit these vulnerabilities. An attacker would have no way to force a user to visit a malicious Web site. Instead, the attacker would have to lure them there, typically by getting them to click a link that takes them to the attacker's site.

\* By default, Outlook Express 6.0, Outlook 2002 and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed. The risk of attack from the HTML email vector can be significantly reduced if the following conditions are met:

\* You have applied the patch included with Microsoft Security bulletin MS03-040

\* You are using Internet Explorer 6 or later

\* You are using the Microsoft Outlook Email Security Update or Microsoft Outlook Express 6.0 and higher, or Microsoft Outlook 2000 or higher in their default configuration.

\* If an attacker exploited these vulnerabilities, they would gain only the same privileges as the user. Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges.

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS03-048)

In addition, there are two individual mitigating factors for the XML Object Vulnerability:

- \* A Web page that tried to exploit this vulnerability would present the user with a prompt to download an HTML file. An attacker could only access files on the user's system if the user accepted this prompt.
- \* An attacker can only access files that are in a known location on the user's system.

ADDITIONAL INFORMATION

The complete advisory can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-048.asp>>  
<http://www.microsoft.com/technet/security/bulletin/MS03-048.asp>.

The information has been provided by Microsoft Product Security.

=====

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.