

# [NT] Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00009.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 13 Sep 2006 08:55:42 +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>

-----

Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

---

## SUMMARY

There is an information disclosure vulnerability in the Indexing Service because of the way that it handles query validation. The vulnerability could allow an attacker to run client-side script on behalf of a user. The script could spoof content, disclose information, or take any action that the user could take on the affected Web site.

## DETAILS

Affected Software:

\* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=778294ae-c5e3-4f17-b0e4-308e46e00105>>

Download the update

\* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2731c0bf-6034-4c16-bb57-66e70a31a3d6>>

Download the update

\* Microsoft Windows XP Professional x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3f604b2a-1383-4a45-b25b-c468deefbfc1>>

Download the update

## [NT] Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

\* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service

Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0182e8e7-9755-46cc-a393-c1e95fd508b2>>

Download the update

\* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft

Windows Server 2003 with SP1 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=e3e4a66c-ca9d-453b-8875-fb57528117ac>>

Download the update

\* Microsoft Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=acf35f34-0d26-4b79-b81f-1111a784a66d>>

Download the update

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0032>>

CVE-2006-0032

Mitigating Factors for Microsoft Indexing Service Vulnerability –

CVE-2006-0032:

\* By default, Internet Information Services (IIS) is not installed on Windows XP or on Windows Server 2003.

\* On Windows Server 2003, the Indexing Service is not enabled by default.

\* On Windows Server 2003, even when the Indexing Service is installed, by default it is not accessible from IIS. Manual steps are required to enable IIS to become a Web-based interface for the Indexing Service. By default the Indexing Service is used only to perform local and remote file system queries.

Workarounds for Microsoft Indexing Service Vulnerability – CVE-2006-0032:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

\* Do not browse the Internet from a system in a server role

Do not browse the Internet from a Web server or a system in any other server role.

\* Disable page encoding auto-detection in Internet Explorer

Disabling the page encoding auto-detection in Internet Explorer helps protect the affected system from attempts to exploit this vulnerability.

To configure components and services:

1. Launch Internet Explorer.

2. Click on View, click Encoding, if Auto-select has a check mark next to it, and left click Auto-select to de-select this setting.

Impact of Workaround: Internet Explorer may fail to properly detect the encoding used on web pages that do not specify a default character encoding, resulting in encoded characters being displayed incorrectly. The user can still manually select the proper encoding type to display the page properly.

## [NT] Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

\* Use URLScan on Windows 2000 running IIS 5.0

The installation of

<<http://www.microsoft.com/technet/security/tools/urlscan.msp>> URLScan helps protect the affected system from attempts to exploit this vulnerability.

1. Install URLScan, in its default configuration URLScan 2.5 will block requests for .IDA, .IDQ and .HTW files which are the affected Index Server extensions.
2. Restart the IISAdmin and WWW Publishing services for the changes to take effect.

Impact of Workaround: The default configuration of URLScan will block requests for Index Server file types (.IDA, .IDQ, .HTW) and as such will block any web based searches that make use of these file types.

\* Remove the Index Server ISAPI extension Script Mappings from Internet Information Service for Windows 2000 running IIS 5.0

The removal of the Index Server ISAPI extension Script Mappings from IIS helps protect the affected system from attempts to exploit this vulnerability.

1. Click Start, and then click Control Panel. Alternatively, point to Settings, and then click Control Panel
2. Double-click Administrative Tools.
3. Double-click Internet Information Services.
4. Right click WebServer, select Properties.
5. Select within Master Properties, select WWW Service and click Edit.
6. On the WWW ServiceMaster Properties, select Home Directory and click Configuration.
7. On the Application Configuration, highlight the .HTW, .IDA and .IDQ extensions and click Remove.

Impact of Workaround: The default configuration of URLScan will block requests for Index Server file types (.IDA, .IDQ, .HTW) and as such will block any web based searches that make use of these file types.

\* Remove the Indexing Service

If the Indexing Service is no longer needed, you could remove it by following this procedure.

To configure components and services:

1. Click Start, and then click Control Panel. Alternatively, point to Settings, and then click Control Panel.
2. Double-click Add or Remove Programs.
3. Click Add/Remove Windows Components.
4. Click to clear the Indexing Service check box to remove the Indexing Service.
5. Complete the Windows Components Wizard by following the instructions on

[NT] Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

the screen.

Impact of Workaround: If this service is removed, all search functionality is provided by traversing the folder hierarchy and scanning each file for the requested string and search responses will be slower. If the MMC Indexing Service snap-in is used to create a new catalog, the catalog will remain offline until this service is started.

\* Disable the Indexing Service extensions from IIS on Windows 2003 running IIS 6.0

If the Indexing Service extensions are no longer needed, you could disable it by following this procedure.

To configure components and services:

1. Double-click Administrative Tools.
2. Double-click Internet Information Services.
3. Click Web Service Extensions.
4. Click Indexing Service.
5. Click Prohibit.

Impact of Workaround: If this service extension is removed, all search functionality is provided by traversing the folder hierarchy and scanning each file for the requested string and search responses will be slower. If the MMC Indexing Service snap-in is used to create a new catalog, the catalog will remain offline until this service is started.

ADDITIONAL INFORMATION

The information has been provided by Eiji James Yoshida.  
 The original article can be found at:  
 <<http://www.microsoft.com/technet/security/Bulletin/MS06-053.msp>>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-053.msp>

=====

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@xxxxxxxxxxxxxx  
 In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

DISCLAIMER:

[NT] Vulnerability in Indexing Service Allows Cross-Site Scripting (MS06-053)

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.