

[NT] Vulnerability in Internet Information Services Allows Code Execution (MS08-006)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Feb 2008 12:18:30 +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 Internet Information Services Allows Code Execution
(MS08-006)

SUMMARY

This important update resolves a privately reported vulnerability in Internet Information Services (IIS). A remote code execution vulnerability exists in the way that IIS handles input to ASP Web pages. An attacker who successfully exploited this vulnerability could then perform actions on the IIS server with the same rights as the Worker Process Identity (WPI). The WPI is configured with Network Service account privileges by default. IIS servers with ASP pages whose application pools are configured with a WPI that uses an account with administrative privileges could be more seriously impacted than IIS servers whose application pool is configured with the default WPI settings.

The security update is rated important for Microsoft Internet Information Services on all supported editions of Windows XP and Windows Server 2003. For more information, see the subsection, Affected and Non-Affected Software, in this section.

Recommendation. Microsoft recommends that customers apply the update at the earliest opportunity.

[NT] Vulnerability in Internet Information Services Allows Code Execution (MS08-006)

DETAILS

Affected Software

Operating System – Component – Maximum Security Impact – Aggregate

Severity Rating – Bulletins Replaced by this Update

* Windows XP Professional Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=2b498065-d682-4227-b23e-d234d7d6a3fe>>

Microsoft Internet Information Services 5.1 – Remote Code Execution – Important – MS06-034

* Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=df9875f7-04d6-486e-bdb5-35e9e305fa1d>>

Microsoft Internet Information Services 6.0 – Remote Code Execution – Important – MS06-034

* Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=6583e798-d16d-419c-ae1-30c3e6c635b3>>

Microsoft Internet Information Services 6.0 – Remote Code Execution – Important – MS06-034

* Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=e8286174-8209-409f-8805-e534715a741c>>

Microsoft Internet Information Services 6.0 – Remote Code Execution – Important – MS06-034

* Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?familyid=29faa70d-f1ac-4da4-b72a-faf1973cd845>>

Microsoft Internet Information Services 6.0 – Remote Code Execution – Important – MS06-034

Non-Affected Software

* Microsoft Windows 2000 Service Pack 4

* Windows Vista

* Windows Vista x64 Edition

* Windows Vista Service Pack 1 (all editions)

* Windows Server 2008 (all editions)

ASP Vulnerability – CVE-2008-0075

A remote code execution vulnerability exists in the way that Internet Information Services handles input to ASP Web pages. An attacker could exploit the vulnerability by passing malicious input to a Web site's ASP page. An attacker who successfully exploited this vulnerability could then perform any actions on the IIS Server with the same rights as the Worker Process Identity (WPI), which by default is configured with Network Service account privileges.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0075>>

CVE-2008-0075

Mitigating Factors for ASP Vulnerability – CVE-2008-0075

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- * IIS 5.1 is not part of a default install of Windows XP Professional Service Pack 2.
- * On supported editions of Windows Server 2003, IIS is not installed or enabled by default.
- * On supported editions of Windows Server 2003, if IIS is enabled, classic ASP is not installed or enabled by default.
- * On supported editions of Windows Server 2003, if IIS is enabled and classic ASP is used, an attacker who successfully exploited this vulnerability could only obtain Network Service account privileges by default. By default, Network Service account privileges have the same user rights as an authenticated user.
- * ASP.NET is not affected by this vulnerability. Customers who have only ASP.NET installed and not ASP are not at risk from this vulnerability.

Workarounds for ASP Vulnerability – CVE-2008-0075

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- * On Windows Server 2003, disable classic ASP

To disable classic ASP, follow these steps:

1. Click Start, click Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. Click the plus sign (+) next to the server's name and then click the Web Service Extensions folder.
3. Click to highlight Active Server Pages in the right pane and then click Prohibit.

Impact of workaround. Users will be unable to use classic ASP pages.

How to undo the workaround. To undo the workaround, follow steps 1 through 3 above and click Allow when highlighting Active Server Pages.

FAQ for ASP Vulnerability – CVE-2008-0075

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could then perform actions on the IIS server with the same rights as the Worker Process Identity (WPI), which by default is configured with Network Service account privileges.

What causes the vulnerability?

The vulnerability is caused by the way that Internet Information Services incorrectly processes input to ASP pages.

What might an attacker use the vulnerability to do?

[NT] Vulnerability in Internet Information Services Allows Code Execution (MS08-006)

An attacker who successfully exploited this vulnerability could then perform actions on the IIS Server with the same rights as the Worker Process Identity (WPI), which is configured with Network Service account privileges by default. Services configured with Network Service account privileges obtain authenticated user level access, not administrative level access. For more information see NetworkService Account. IIS servers whose application pool is configured with a WPI that uses an account with administrative privileges could be more seriously impacted than IIS servers whose application pool is configured with the default WPI settings.

The Network Service account uses the computer's credentials when it authenticates remotely, but has a greatly reduced privilege level on the server itself and, therefore, does not have local administrator privileges. For more information see NetworkService Account, IIS and Built-in Accounts (IIS 6.0), Configuring Worker Process Identities (IIS 6.0), and Configuring Application Pools in IIS 6.0 (IIS 6.0).

How could an attacker exploit the vulnerability?

An attacker could pass specially crafted input to an ASP page. The ASP page could already exist or could be uploaded by a user in a hosted environment.

What are worker processes for IIS?

Worker processes are processes that execute the server-side processing tasks for a web server. For information on worker processes and how they are implemented in IIS 6.0 see Worker Processes (IIS 6.0). Additional information on worker processes and how they execute Web-based applications in isolation see Worker Process Isolation Mode (IIS 6.0).

What is ASP?

Microsoft Active Server Pages (ASP) is a server-side scripting technology that can be used to create dynamic and interactive Web applications. An ASP page is an HTML page that contains server-side scripts that are processed by the Web server before being sent to the user's browser.

What systems are primarily at risk from the vulnerability?

Windows Server 2003 Web servers are at risk if IIS and ASP are enabled. Web hosting providers that allow their customers to upload ASP pages to their hosted Web sites are at increased risk.

What does the update do?

The update removes the vulnerability by changing the way that Internet Information Services processes input to ASP pages.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

[NT] Vulnerability in Internet Information Services Allows Code Execution (MS08-006)

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms08-006.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms08-006.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:

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.