

[NT] Cumulative Security Update for Internet Explorer (MS08-010)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00057.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2008 09:03:57 +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 (MS08-010)

SUMMARY

This critical security update resolves three privately reported and one publicly reported vulnerabilities. The most serious of the vulnerabilities could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

The security update is rated critical for all supported releases of Internet Explorer. For more information, see the subsection, Affected and Non-Affected Software, in this section.

DETAILS

Affected Software

Operating System – Component – Maximum Security Impact – Aggregate

Severity Rating – Bulletins Replaced by This Update

Internet Explorer 5.01 and Internet Explorer 6 Service Pack 1

* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1032A039-468B-4C5F-8C1C-5E54C2832E41>>

[NT] Cumulative Security Update for Internet Explorer (MS08-010)

Microsoft Internet Explorer 5.01 Service Pack 4 – Remote Code Execution – Critical – MS07-069

* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=87E66DCE-5060-4814-8754-829B4E190359>>

Microsoft Internet Explorer 6 Service Pack 1 – Remote Code Execution – Critical – MS07-069

Internet Explorer 6

* Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=BB2AA3CB-021F-4890-AB20-2A51F8E17554>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8989F576-8B30-4866-90EC-929D24F3B409>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=429B7ED1-FE78-459A-B834-D0F3C69CB703>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E989E23C-38BB-4FE7-A830-D7BDF7659392>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS07-069

* 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=5A097F7A-B696-48D0-B13F-337C5FD14E24>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS07-069

Internet Explorer 7

* Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D4AA293A-6332-4C6C-B128-876F516BD030>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B72AF1B6-6E23-4005-AEF6-82195B380153>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B2AA6562-881E-4FD6-BE1B-53426A0FF4A9>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4BB99AFC-BE14-4F2E-9570-B7FE09E39131>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

* 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=6FA80E2C-5E91-4B33-ACD9-33F156660AE7>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

* Windows Vista –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0DE25B98-F443-4874-A06F-4DAAE14C16B0>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

* Windows Vista x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C08EBBE7-639B-4EA2-8304-FAB531930ABF>>

[NT] Cumulative Security Update for Internet Explorer (MS08-010)

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS07-069

Non-Affected Software

- * Internet Explorer 7 on Windows Vista Service Pack 1 (all editions)
- * Internet Explorer 7 on Windows Server 2008 (all editions)

HTML Rendering Memory Corruption Vulnerability – CVE-2008-0076

A remote code execution vulnerability exists in the way Internet Explorer interprets HTML with certain layout combinations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0076>>
CVE-2008-0076

Property Memory Corruption Vulnerability – CVE-2008-0077

A remote code execution vulnerability exists in the way Internet Explorer handles a property method. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0077>>
CVE-2008-0077

Argument Handling Memory Corruption Vulnerability – CVE-2008-0078

A remote code execution vulnerability exists in the way Internet Explorer handles argument validation in image processing. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0078>>
CVE-2008-0078

ActiveX Object Memory Corruption Vulnerability – CVE-2007-4790

A remote code execution vulnerability exists in a component of Microsoft Fox Pro. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

CVE Information:

[NT] Cumulative Security Update for Internet Explorer (MS08-010)

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4790>>
CVE-2007-4790

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/ms08-010.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms08-010.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.