

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-11/msg00027.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 12 Nov 2008 18:02:52 +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>

Vulnerabilities in Microsoft XML Core Services Allow Code Execution
(MS08-069)

SUMMARY

This security update resolves several vulnerabilities in Microsoft XML Core Services. The most severe vulnerability 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.

This security update is rated Critical for Microsoft XML Core Services 3.0 and Important for Microsoft XML Core Services 4.0, Microsoft XML Core Services 5.0, and Microsoft XML Core Services 6.0. For more information, see the subsection, Affected and Non-Affected Software, in this section.

DETAILS

Affected Software:

Windows 2000

* Microsoft Windows 2000 Service Pack 4 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07-042

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08–069)

- * Microsoft Windows 2000 Service Pack 4 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Important – MS07–042
- * Microsoft Windows 2000 Service Pack 4 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – MS07–042

Windows XP

- * Windows XP Service Pack 2 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07–042
- * Windows XP Service Pack 3 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows XP Service Pack 2 and Windows XP Service Pack 3 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Important – MS07–042
- * Windows XP Service Pack 2 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – MS07–042
- * Windows XP Service Pack 3 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – None
- * Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07–042
- * Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Important – MS07–042
- * Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – MS07–042

Windows Server 2003

- * Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07–042
- * Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Low – MS07–042
- * Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – MS07–042
- * Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07–042
- * Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Low – MS07–042
- * Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – MS07–042
- * Windows Server 2003 with SP1 for Itanium–based Systems and Windows Server 2003 with SP2 for Itanium–based Systems – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07–042
- * Windows Server 2003 with SP1 for Itanium–based Systems and Windows Server 2003 with SP2 for Itanium–based Systems – Microsoft XML Core

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)

Services 4.0 (KB954430) – Information Disclosure – Low – MS07-042

- * Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – MS07-042

Windows Vista

- * Windows Vista – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07-042
- * Windows Vista Service Pack 1 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows Vista and Windows Vista Service Pack 1 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Important – MS07-042
- * Windows Vista – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – MS07-042
- * Windows Vista Service Pack 1 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – None
- * Windows Vista x64 Edition – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – MS07-042
- * Windows Vista x64 Edition Service Pack 1 – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1 – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Important – MS07-042
- * Windows Vista x64 Edition – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – MS07-042
- * Windows Vista x64 Edition Service Pack 1 – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Important – None

Windows Server 2008

- * Windows Server 2008 for 32-bit Systems – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows Server 2008 for 32-bit Systems – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Low – MS07-042
- * Windows Server 2008 for 32-bit Systems – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – None
- * Windows Server 2008 for x64-based Systems – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows Server 2008 for x64-based Systems – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Low – MS07-042
- * Windows Server 2008 for x64-based Systems – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – None
- * Windows Server 2008 for Itanium-based Systems – Microsoft XML Core Services 3.0 (KB955069) – Remote Code Execution – Critical – None
- * Windows Server 2008 for Itanium-based Systems – Microsoft XML Core Services 4.0 (KB954430) – Information Disclosure – Low – MS07-042
- * Windows Server 2008 for Itanium-based Systems – Microsoft XML Core Services 6.0 (KB954459) – Information Disclosure – Low – None

Microsoft Office

- * Microsoft Office 2003 Service Pack 3 – Microsoft XML Core Services 5.0 (KB951535) – Information Disclosure – Important – None

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)

- * Microsoft Word Viewer 2003 Service Pack 3 – Microsoft XML Core Services 5.0 (KB951535) – Information Disclosure – Important – None
- * 2007 Microsoft Office System – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – MS07-042
- * 2007 Microsoft Office System Service Pack 1 – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – None
- * Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – MS07-042
- * Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – None
- * Microsoft Expression Web – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – MS07-042
- * Microsoft Expression Web 2 – Microsoft XML Core Services 5.0 (KB951550) – Information Disclosure – Important – None
- * Microsoft Office SharePoint Server 2007 (32-bit editions) – Microsoft XML Core Services 5.0 (KB951597) – Information Disclosure – Important – MS07-042
- * Microsoft Office SharePoint Server 2007 Service Pack 1 (32-bit editions) – Microsoft XML Core Services 5.0 (KB951597) – Information Disclosure – Important – None
- * Microsoft Office SharePoint Server 2007 and Microsoft Office SharePoint Server 2007 Service Pack 1 (64-bit editions) – Microsoft XML Core Services 5.0 (KB951597) – Information Disclosure – Important – None
- * Microsoft Office Groove Server 2007 – Microsoft XML Core Services 5.0 (KB951597) – Information Disclosure – Important – MS07-042

Non-Affected Software:

- * Microsoft Office 2000 Service Pack 3
- * Microsoft Office XP Service Pack 3
- * Microsoft Office SharePoint Portal Server 2001 Service Pack 3
- * Microsoft Office SharePoint Portal Server 2003 Service Pack 3
- * Microsoft Excel Viewer 2003 Service Pack 3

MSXML Memory Corruption Vulnerability – CVE-2007-0099:

A remote code execution vulnerability exists in the way that Microsoft XML Core Services parses XML content. The vulnerability could allow remote code execution if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0099>>
CVE-2007-0099

MSXML DTD Cross-Domain Scripting Vulnerability – CVE-2008-4029

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)

An information disclosure vulnerability exists in the way that Microsoft XML Core Services handles error checks for external document type definitions (DTDs). The vulnerability could allow information disclosure if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. An attacker who successfully exploited this vulnerability could read data from a Web page in another domain in Internet Explorer. In all cases, however, an attacker would have no way to force users to visit these Web sites.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4029>>
CVE-2008-4029

MSXML Header Request Vulnerability – CVE-2008-4033

An information disclosure vulnerability exists in the way that Microsoft XML Core Services handles transfer-encoding headers. The vulnerability could allow information disclosure if a user browses a Web site that contains specially crafted content or opens specially crafted HTML e-mail. An attacker who successfully exploited this vulnerability could read data from a Web page in another domain in Internet Explorer. In all cases, however, an attacker would have no way to force users to visit these Web sites.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4033>>
CVE-2008-4033

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/ms08-069.msp>>
<http://www.microsoft.com/technet/security/bulletin/ms08-069.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@xxxxxxxxxxxxxxxxx

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

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

[NT] Vulnerabilities in Microsoft XML Core Services Allow Code Execution (MS08-069)

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.