

# [NT] Vulnerabilities in Microsoft Office Web Components Allows Code Execution (MS08-017)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00042.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 12 Mar 2008 15:42:28 +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 Office Web Components Allows Code Execution  
(MS08-017)

---

## SUMMARY

This critical update resolves two privately reported vulnerabilities in Microsoft Office Web Components. These vulnerabilities could allow remote code execution if a user viewed a specially crafted Web page. 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.

This is a critical security update for implementations of Microsoft Office Web Components 2000 on supported editions of Microsoft Office 2000 Service Pack 3, Microsoft Office XP Service Pack 3, Visual Studio .NET 2002 Service Pack 1, Visual Studio .NET 2003 Service Pack 1, Microsoft BizTalk Server 2000 and Microsoft BizTalk Server 2002, Microsoft Commerce Server 2000, and Internet Security and Acceleration Server 2000 Service Pack 2. For more information, see the subsection, Affected and Non-Affected Software, in this section.

## DETAILS

### Affected Software:

Office Suite and Other Software – Component – Maximum Security Impact –

Aggregate Severity Rating – Bulletins Replaced by this Update

Client

\* Microsoft Office 2000 Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=806c654a-35e3-4385-855a-4b803249bfcf>>

Microsoft Office Web Components 2000 (KB931660) – Remote Code Execution – Critical – None

\* Microsoft Office XP Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=f54d2a5e-c0ed-4f70-9746-38dd61c8e9d7>>

Microsoft Office Web Components 2000 (KB932031) – Remote Code Execution – Critical – None

\* Visual Studio .NET 2002 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D71B23FA-A873-406D-BAD7-E38E565DEE39>>

Microsoft Office Web Components 2000 (KB933367) – Remote Code Execution – Critical – None

\* Visual Studio .NET 2003 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2FE10CCD-40CB-4090-B83D-EAE3D4ECA174>>

Microsoft Office Web Components 2000 (KB933369) – Remote Code Execution – Critical – None

### Server

\* Microsoft BizTalk Server 2000 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5FDDDD54F-7A33-4EA3-B68D-B96A9BAE509D>>

Microsoft Office Web Components 2000 (KB939714) – Remote Code Execution – Critical – None

\* Microsoft BizTalk Server 2002 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5FDDDD54F-7A33-4EA3-B68D-B96A9BAE509D>>

Microsoft Office Web Components 2000 (KB939714) – Remote Code Execution – Critical – None

\* Microsoft Commerce Server 2000 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=71DE76BA-B62C-4A7A-A78A-9317F5255B13>>

Microsoft Office Web Components 2000 (KB941305) – Remote Code Execution – Critical – None

\* Internet Security and Acceleration Server 2000 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=526D87BD-C3DA-412E-8765-C15987AE9B01>>

Microsoft Office Web Components 2000 (KB948257) – Remote Code Execution – Critical – None

### Non-Affected Software:

\* Office Suite

\* Microsoft Works 8

\* Microsoft Works 9

\* Microsoft Works Suite 2005

\* Microsoft Works Suite 2006

\* Microsoft Office 2003 Service Pack 2

\* Microsoft Office 2003 Service Pack 3

\* 2007 Microsoft Office System

\* 2007 Microsoft Office System Service Pack 1

\* Microsoft BizTalk Server 2004

## [NT] Vulnerabilities in Microsoft Office Web Components Allows Code Execution (MS08-017)

- \* Microsoft BizTalk Server 2006
- \* Microsoft Commerce Server 2000 Service Pack 1, Microsoft Commerce Server 2000 Service Pack 2, and Microsoft Commerce Server 2000 Service Pack 3
- \* Microsoft Commerce Server 2002
- \* Microsoft Commerce Server 2007
- \* Internet Security and Acceleration Server 2004
- \* Internet Security and Acceleration Server 2006

### Office Web Components URL Parsing Vulnerability – CVE-2006-4695

A remote code execution vulnerability exists in the way Microsoft Office Web Components manages memory resources when parsing specially crafted URLs. 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. 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.

#### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4695>>  
CVE-2006-4695

### Office Web Components DataSource Vulnerability – CVE-2007-1201

A remote code execution vulnerability exists in the way Microsoft Office Web Components manages memory resources. 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. 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.

#### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1201>>  
CVE-2007-1201

#### Workarounds:

- \* Prevent Office Web Components Library from running in Internet Explorer.

You can prevent the Office Web Components Library from running in Internet Explorer by setting the kill bit for the control in the registry.

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.

Microsoft cannot guarantee that you can solve problems that result from

## [NT] Vulnerabilities in Microsoft Office Web Components Allows Code Execution (MS08-017)

using Registry Editor incorrectly. Use the Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

For detailed steps that you can use to prevent a control from running in Office Web Components, see Microsoft Knowledge Base Article 240797. Follow these steps in this article to create a Compatibility Flags value in the registry to prevent the Office Web Components library from running.

Note The Class Identifiers and corresponding files where the library objects are contained are documented in the FAQ What does the update do? Replace {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX} below with the Class Identifiers found in this section.

\* To set the kill bit for a CLSID with a value of {0002E533-0000-0000-C000-000000000046}, paste the following text in a text editor such as Notepad. Then, save the file by using the .reg file name extension.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{ 0002E533-0000-0000-C000-000000000046}]  
"Compatibility Flags"=dword:00000400
```

\* To set the kill bit for a CLSID with a value of {0002E530-0000-0000-C000-000000000046}, paste the following text in a text editor such as Notepad. Then, save the file by using the .reg file name extension.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{0002E530-0000-0000-C000-000000000046}]  
"Compatibility Flags"=dword:00000400
```

You can apply this .reg file to individual systems by double-clicking it. You can also apply it across domains by using Group Policy. For more information about Group Policy, visit the following Microsoft Web sites:

\*

[http://technet2.microsoft.com/WindowsServer/en/library/6d7cb788-b31d-4d17-9f1e-b5ddaa6deecd1033.msp?mfr=Group Policy Collection](http://technet2.microsoft.com/WindowsServer/en/library/6d7cb788-b31d-4d17-9f1e-b5ddaa6deecd1033.msp?mfr=Group%20Policy%20Collection)

\* What is

[http://technet2.microsoft.com/windowsserver/en/library/47ba1311-6cca-414f-98c9-2d7f99fca8a31033.msp?mfr=Group Policy Object Editor?](http://technet2.microsoft.com/windowsserver/en/library/47ba1311-6cca-414f-98c9-2d7f99fca8a31033.msp?mfr=Group%20Policy%20Object%20Editor?)

\* Core

## [NT] Vulnerabilities in Microsoft Office Web Components Allows Code Execution (MS08-017)

<<http://technet2.microsoft.com/windowsserver/en/library/e926577a-5619-4912-b5d9-e73d4bdc94911033.mspx?mfr>  
Group Policy Tools and Settings

Note You must restart Internet Explorer for your changes to take effect.

Impact of Workaround: Applications requiring Office Web Components functionality will not function.

How to undo the Workaround: You can undo the workaround documented above by following these steps:

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use the Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

\* To undo the kill bit for a CLSID with a value of {0002E510-0000-0000-C000-000000000046}, paste the following text in a text editor such as Notepad. Then, save the file by using the .reg file name extension.

Windows Registry Editor Version 5.00

```
CLSID_OWC9_DataSourceControl, {0002E533-0000-0000-C000-000000000046}
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{0002E533-0000-0000-C000-000000000046}]
```

```
CLSID_OWC9_DataSourceControl, {0002E530-0000-0000-C000-000000000046}
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{0002E530-0000-0000-C000-000000000046}]
```

\* Unregister the Office Web Components 2000 Library

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use the Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

\* For Office 2000, type the following at the command prompt and select

[NT] Vulnerabilities in Microsoft Office Web Components Allows Code Execution (MS08-017)

Run:

```
Regsvr32.exe /u "C:\Program Files\Microsoft Office\Office\MSOWC.DLL"
```

\* For Office XP, type the following at the command prompt and select Run:

```
Regsvr32.exe /u "C:\Program Files\Microsoft Office\Office\MSOWC.DLL"
```

Impact of Workaround: Applications requiring Office Web Components functionality will not function.

How to undo the Workaround: To re-register the Office Web Components 2000, follow these steps:

\* For Office 2000, type the following at the command prompt and select Run:

```
Regsvr32.exe "C:\Program Files\Microsoft Office\Office\MSOWC.DLL"
```

\* For Office XP, type the following at the command prompt and select Run:

```
Regsvr32.exe "C:\Program Files\Microsoft Office\Office\MSOWC.DLL"
```

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/MS08-017.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS08-017.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@xxxxxxxxxxxxxxxx

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

=====

=====

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.