Security Bulletin

Microsoft Security Bulletin MS12-046 - Important

Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution (2707960)

Published: July 10, 2012 | Updated: November 13, 2012

Version: 2.0

General Information

Executive Summary

This security update resolves one publicly disclosed vulnerability in Microsoft Visual Basic for Applications. The vulnerability could allow remote code execution if a user opens a legitimate Microsoft Office file (such as a .docx file) that is located in the same directory as a specially crafted dynamic link library (DLL) file. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. 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 Important for all supported versions of Microsoft Visual Basic for Applications SDK and third-party applications that use Microsoft Visual Basic for Applications. This security update is also rated Important for all supported editions of Microsoft Office 2003 SP3, Microsoft Office 2007 SP2, and Microsoft Office 2010. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting how Microsoft Visual Basic for Applications loads external libraries. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Customers can configure automatic updating to check online for updates from Microsoft Update by using the Microsoft Update service. Customers who have automatic updating enabled and configured to check online for updates from Microsoft Update typically will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates from Microsoft Update and install this update manually. For information about specific configuration options in automatic updating in supported editions of Windows XP and Windows Server 2003, see Microsoft Knowledge Base Article 294871. For information about automatic updating in supported editions of Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, see Understanding Windows automatic updating.

For administrators and enterprise installations, or end users who want to install this security update manually, Microsoft recommends that customers apply the update at the earliest opportunity using update management software, or by checking for updates using the Microsoft Update service.

See also the section, **Detection and Deployment Tools and Guidance**, later in this bulletin.

Known Issues. Microsoft Knowledge Base Article 2707960 documents the currently known issues that customers may experience when installing this security update. The article also documents recommended solutions for these issues. When currently known issues and recommended solutions pertain only to specific releases of this software, this article provides links to further articles.

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Microsoft Office Suites and Software

Expand table

Office Software	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office 2003 Service Pack 3 [1] \ (KB2687626)	Remote Code Execution	Important	KB976382 in MS10-031 replaced by KB2598361 or KB2687626[2]
Microsoft Office 2007 Service Pack 2 [1] \ (KB2596744)	Remote Code Execution	Important	KB976321 in MS10-031 replaced by KB2596744
Microsoft Office 2007 Service Pack 3 [1] \ (KB2596744)	Remote Code Execution	Important	None
Microsoft Office 2010 (32-bit editions) \ (KB2598243)\ \ Microsoft Office 2010 (32-bit editions) \ (KB2553447)	Remote Code Execution	Important	None
Microsoft Office 2010 Service Pack 1 (32-bit editions) \ (KB2598243)\ \ Microsoft Office 2010 Service Pack 1 (32-bit editions) \ (KB2553447)	Remote Code Execution	Important	None
Microsoft Office 2010 (64-bit editions) \ (KB2598243)\ \ Microsoft Office 2010 (64-bit editions) \ (KB2553447)	Remote Code Execution	Important	None
Microsoft Office 2010 Service Pack 1 (64-bit editions) \ (KB2598243)\ \ Microsoft Office 2010 Service Pack 1 (64-bit editions) \ (KB2553447)	Remote Code Execution	Important	None

[1]These updates for Microsoft Office apply to all supported Microsoft Office suites and other Microsoft Office software that contain the vulnerable shared Office component. These include, but are not limited to, supported versions of Microsoft Visio and Microsoft Project. For more information, see the next section, **Frequently Asked Questions (FAQ) Related to This Security Update**.

[2]Although the rereleased update (KB2687626) replaces the original update (KB2598361) for Microsoft Office 2003 Service Pack 3, customers who have successfully installed the KB2598361 update do not need to install the KB2687626 update. For more information, see the update FAQ.

Microsoft Developer Tools and Software

Expand table

Software	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Visual Basic for Applications [1]\ (KB2688865)	Remote Code Execution	Important	KB974945 in MS10-031 replaced by KB2688865
Microsoft Visual Basic for Applications SDK[2][3]	Remote Code Execution	Important	None

[1]This update package applies to supported versions of the Microsoft Visual Basic for Applications runtime (Vbe6.dll) and is available from the Microsoft Download Center only.

[2]The supported versions of the VBA SDK are Microsoft Visual Basic for Applications SDK 6.3, Microsoft Visual Basic for Applications SDK 6.4, and Microsoft Visual Basic for Applications SDK 6.5.

[3]The updated version of the Visual Basic for Applications SDK that addresses the vulnerability described in this bulletin is available for independent software vendors (ISVs) from the Summit Software Company. For more information, see the next section, **Frequently Asked Questions (FAQ) Related to This Security Update**.

Non-Affected Software

Expand table

Office and Other Software
Microsoft Office 2008 for Mac
Microsoft Office for Mac 2011
Microsoft Office Compatibility Pack Service Pack 2 and Microsoft Office Compatibility Pack Service Pack 3
Microsoft Excel Viewer
Microsoft Word Viewer
Microsoft PowerPoint Viewer
Microsoft Visio Viewer 2010 and Microsoft Visio Viewer 2010 Service Pack 1

Frequently Asked Questions (FAQ) Related to This Security Update

Why was this bulletin revised on November 13, 2012?
Microsoft rereleased this bulletin to replace the KB2598361 update with the KB2687626 update for Microsoft Office 2003 Service Pack 3 to address an issue involving specific digital certificates that were generated by Microsoft without proper timestamp attributes. For more information, see Microsoft Security Advisory 2749655.

Although the rereleased update (KB2687626) replaces the original update (KB2598361) for Microsoft Office 2003 Service Pack 3, customers who have successfully installed the KB2598361 update do not need to install the KB2687626 update.

I have already successfully installed the original KB2598361 update for Microsoft Office 2003. Do I need to apply the rereleased update package (KB2687626) released on November 13, 2012?
No. The rereleased update (KB2687626) only applies to systems running Microsoft Office 2003 on which the original update (KB2598361) has not been installed. Customers who have already successfully installed the original KB2598361 update for Microsoft Office 2003 Service Pack 3 do not need to take any action. In addition, customers will not be offered the rereleased update (KB2687626) if the original update (KB2598361) is already installed on their systems.

Note In the case where the KB2598361 update is already installed, and then the KB2687626 update is installed on the same system, the installer generates a message that the update is already installed. After the message is generated, the KB2687626 update will replace the KB2598361 update in the list of installed updates. For more information about this installation behavior, see Microsoft Knowledge Base Article 2707960.

Is this update related to Microsoft Security Advisory 2269637?
Yes, the Visual Basic for Applications Insecure Library Loading Vulnerability (CVE-2012-1854) addressed by this update is related to the class of vulnerabilities, described in Microsoft Security Advisory 2269637, that affects how applications load external libraries. This security update addresses a particular instance of this type of vulnerability.

The update is to a shared component used by Microsoft Office. Will the update be offered to Microsoft Office software that includes the shared component, even if the software does not

access the vulnerable code?

Yes, the update will be offered to systems where the vulnerable shared Office component is detected. This is true even for cases where the Office software includes VBE6.dll but does not access the vulnerable code.

Why are multiple package updates available for Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1?

The updates required to address the vulnerability described in this bulletin are offered across different package updates as indicated in the **Affected Software** table due to the componentized servicing model for Microsoft Office 2010. To be protected from the vulnerability, both updates are required, but they do not need to be installed in a particular order.

Where are the file information details?

Refer to the reference tables in the **Security Update Deployment** section for the location of the file information details.

Where are the hashes of the security updates?

The SHA1 and SHA2 hashes of the security updates can be used to verify the authenticity of downloaded security update packages. For the hash information pertaining to this update, see Microsoft Knowledge Base Article 2707960.

I have applied the required Microsoft security updates, but I still have an affected version of the Visual Basic for Applications runtime (VBE6.dll) on my system. How do I update this DLL?

There are cases where your system might still have an affected version of VBE6.dll even after you have installed the required security updates for Microsoft Office and the update for Microsoft Visual Basic for Applications listed in this bulletin.

If VBE6.dll was installed on your system by a supported version of Microsoft Office, then applying the security update for the affected version of Microsoft Office will replace VBE6.dll with the updated version that addresses the vulnerability described in this bulletin. However, if VBE6.dll was installed on your system by a third-party application, you may have to install an update for that program.

To update VBE6.dll for third-party applications there are two possible scenarios depending on the third-party application's implementation of VBA. If you know that the third-party application is compliant to the recommended best practices for using a shared component as a side-by-side assembly, then applying the Microsoft Visual Basic for Applications (KB2688865) update will

replace VBE6.dll in the shared location with the updated version that addresses the vulnerability described in this bulletin.

On the other hand, if the third-party application does not put VBE6.dll in the shared location as per recommended best practices, then you should contact the third-party application developer and ask them to provide you with an updated version of their application that contains a newer version of the VBE6.dll that addresses the vulnerability described in this bulletin.

This security update only applies to Microsoft software. How can I detect if third-party applications have deployed an affected version of the Visual Basic for Applications runtime (VBE6.dll) on my system?

Third-party applications that support VBA could deploy VBE6.dll in a location that is not updated by this security update. In the case that you do have a third-party application that has shipped with its own copy of VBE6.dll, to help ensure that your system is fully protected from the vulnerability described in this bulletin, you should contact the developer or vendor responsible for support for the third-party application directly.

For details on how to scan for copies of VBE6.dll on your system, see Microsoft Knowledge Base Article 978213. Scanning for all copies of VBE6.dll on your system can assist in identifying potentially vulnerable copies that may have been installed by third-party applications.

I am a third-party softwaredeveloper and I use Microsoft Visual Basic for Applications runtime in my application. Is my application vulnerable and how do I update it?

Developers who redistribute the Microsoft Visual Basic for Applications runtime VBE6.dll should download an updated version of the Microsoft Visual Basic for Applications SDK from the Summit Software Company. Then, update the application installer with the updated VBA runtime. For more information on best practices on redistributed component use, please see Microsoft Knowledge Base Article 835322 and the MSDN article, Isolated Applications and Side-by-side Assemblies.

I am an ISV. Where is the update for Microsoft Visual Basic for Applications SDK?

The update is available from the Summit Software Company. Summit Software Company is a global supplier of application customization software products and integration support services to independent software vendors (ISVs) and corporate developers. In June 1996, Summit Software entered into an agreement with Microsoft to sell Microsoft Visual Basic for Applications and related value-added technology and services. Summit continues to sell and support Microsoft VBA.

How areMicrosoft Office standalone programs affected by the vulnerability?
A Microsoft Office standalone program is affected with the same severity rating as the corresponding component in a Microsoft Office Suite. For example, a standalone installation of Microsoft Excel is affected with the same severity rating as an installation of Microsoft Excel that was delivered with a Microsoft Office Suite.

I am using an older release of the software discussed in this security bulletin. What should I do?
The affected software listed in this bulletin have been tested to determine which releases are affected. Other releases are past their support life cycle. For more information about the product lifecycle, visit the Microsoft Support Lifecycle website.

It should be a priority for customers who have older releases of the software to migrate to supported releases to prevent potential exposure to vulnerabilities. To determine the support lifecycle for your software release, see Select a Product for Lifecycle Information. For more information about service packs for these software releases, see Service Pack Lifecycle Support Policy.

Customers who require custom support for older software must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. Customers without an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the Microsoft Worldwide Information website, select the country in the Contact Information list, and then click **Go** to see a list of telephone numbers. When you call, ask to speak with the local Premier Support sales manager. For more information, see the Microsoft Support Lifecycle Policy FAQ.

Vulnerability Information

Severity Ratings and Vulnerability Identifiers

The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the July bulletin summary. For more information, see Microsoft Exploitability Index.

Expand table

Affected Software	Visual Basic for Applications Insecure Library Loading Vulnerability - CVE-2012-1854	Aggregate Severity Rating
Office Suite		
Microsoft Office 2003 Service Pack 3	**Important** Remote Code Execution	**Important**
Microsoft Office 2007 Service Pack 2	**Important** Remote Code Execution	**Important**
Microsoft Office 2007 Service Pack 3	**Important** Remote Code Execution	**Important**
Microsoft Office 2010 (32-bit editions)	**Important** Remote Code Execution	**Important**
Microsoft Office 2010 Service Pack 1 (32-bit editions)	**Important** Remote Code Execution	**Important**
Microsoft Office 2010 (64-bit editions)	**Important** Remote Code Execution	**Important**
Microsoft Office 2010 Service Pack 1 (64-bit editions)	**Important** Remote Code Execution	**Important**
Developer Tools		
Microsoft Visual Basic for Applications[1]	**Important** Remote Code Execution	**Important**
Microsoft Visual Basic for Applications SDK[2]	**Important** Remote Code Execution	**Important**

[1]This update package applies to supported versions of the Microsoft Visual Basic for Applications runtime (Vbe6.dll) and is available from the Microsoft Download Center only.

[2]The supported versions of the VBA SDK are Microsoft Visual Basic for Applications SDK 6.3, Microsoft Visual Basic for Applications SDK 6.4, and Microsoft Visual Basic for Applications SDK 6.5.

Visual Basic for Applications Insecure Library Loading Vulnerability - CVE-2012-1854

A remote code execution vulnerability exists in the way that Microsoft Visual Basic for Applications handles the loading of DLL files. 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.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2012-1854.

Mitigating Factors for Visual Basic for Applications Insecure Library Loading Vulnerability - CVE-2012-1854

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:

- The file sharing protocol, Server Message Block (SMB), is often disabled on the perimeter firewall. This limits the potential attack vectors for this vulnerability.
- For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a legitimate Office-related file (such as a .docx file).
- 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.

Workarounds for Visual Basic for Applications Insecure Library Loading Vulnerability - CVE-2012-1854

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:

- **Disable loading of libraries from WebDAV and remote network shares**

  Note See Microsoft Knowledge Base Article 2264107 to deploy a workaround tool that allows customers to disable the loading of libraries from remote network or WebDAV shares. This tool can be configured to disallow insecure loading on a per-application or a global system basis.

Customers who are informed by their vendor of an application being vulnerable can use this tool to help protect against attempts to exploit this issue.

Note See Microsoft Knowledge Base Article 2264107 to use the automated **Microsoft Fix it** solution to deploy the registry key to block the loading of libraries for SMB and WebDAV shares. Note that this Fix it solution does require you to install the workaround tool also described in Microsoft Knowledge Base Article 2264107 first. This Fix it solution only deploys the registry key and requires the workaround tool in order to be effective. We recommend that administrators review the KB article closely prior to deploying this Fix it solution.

- **Disable the WebClient service**

  Disabling the WebClient service helps protect affected systems from attempts to exploit this vulnerability by blocking the most likely remote attack vector through the Web Distributed Authoring and Versioning (WebDAV) client service. After applying this workaround, remote attackers who successfully exploit this vulnerability may cause the system to run programs located on the targeted user's computer or the Local Area Network (LAN). However, users will be prompted for confirmation before opening arbitrary programs from the Internet.

  To disable the WebClient Service, follow these steps:

  1. Click **Start**, click **Run**, type **Services.msc** and then click **OK**.
  2. Right-click **WebClient** service and select **Properties**.
  3. Change the Startup type to **Disabled**. If the service is running, click **Stop**.
  4. Click **OK** and exit the management application.

  Impact of workaround. When the WebClient service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted. In addition, any services that explicitly depend on the Web Client service will not start, and an error message will be logged in the System log. For example, WebDAV shares will be inaccessible from the client computer.

  How to undo the workaround.

  To re-enable the WebClient Service, follow these steps:

  1. Click **Start**, click **Run**, type **Services.msc** and then click **OK**.

2. Right-click **WebClient** service and select **Properties**.
3. Change the Startup type to **Automatic**. If the service is not running, click **Start**.
4. Click **OK** and exit the management application.

- **Block TCP ports 139 and 445 at the firewall**

  These ports are used to initiate a connection with the affected component. Blocking TCP ports 139 and 445 at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. Microsoft recommends that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, see the TechNet article, TCP and UDP Port Assignments.

  Impact of workaround. Several Windows services use the affected ports. Blocking connectivity to the ports may cause various applications or services to not function. The following is a list of some of the applications or services that could be impacted:
  - Applications that use SMB (CIFS)
  - Applications that use mailslots or named pipes (RPC over SMB)
  - Server (File and Print Sharing)
  - Group Policy
  - Net Logon
  - Distributed File System (DFS)
  - Terminal Server Licensing
  - Print Spooler
  - Computer Browser
  - Remote Procedure Call Locator
  - Fax Service
  - Indexing Service
  - Performance Logs and Alerts
  - Systems Management Server
  - License Logging Service

  How to undo the workaround. Unblock TCP ports 139 and 445 at the firewall. For more information about ports, see TCP and UDP Port Assignments.

FAQ for Visual Basic for Applications Insecure Library Loading Vulnerability - CVE-2012-1854

What is the scope of the vulnerability?

This is a remote code execution vulnerability in Microsoft Visual Basic for Applications (VBA).

What causes the vulnerability?

The vulnerability is caused when Microsoft Visual Basic for Applications incorrectly restricts the path used for loading external libraries.

What is Visual Basic for Applications (VBA)?

Microsoft VBA is a development technology for developing client desktop packaged applications and integrating them with existing data and systems. Microsoft VBA is based on the Microsoft Visual Basic development system. Microsoft Office products include VBA and use VBA to perform certain functions. VBA can also be used to build customized applications based around an existing host application.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain the same user rights as a logged-on user. If the user is logged on with administrative user rights, 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.

How could an attacker exploit the vulnerability?

An attacker could convince a user to open a legitimate Microsoft Office-related file (such as a .docx file) that is located in the same network directory as a specially crafted dynamic link library (DLL) file. Then, while opening the legitimate file, Microsoft Office could attempt to load the DLL file and execute any code it contained.

In an email attack scenario, an attacker could exploit the vulnerability by sending a legitimate Microsoft Office-related file (such as a .docx file) to a user, and convincing the user to put the attachment into a directory that contains a specially crafted DLL file and to open the legitimate file. Then, while opening the legitimate file, Microsoft Office could attempt to load the DLL file and execute any code it contained.

In a network attack scenario, an attacker could put a legitimate Microsoft Office-related file and a specially crafted DLL file in a network share, a UNC, or WebDAV location and then convince the user to open the file.

What systems are primarily at risk from the vulnerability?

Systems where Microsoft Office is used, including workstations and terminal servers, are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do?

The update addresses this vulnerability by correcting how Microsoft Visual Basic for Applications loads external libraries.

Is this vulnerability related to Microsoft Security Advisory 2269637?

Yes. This vulnerability is related to the class of vulnerabilities described in Microsoft Security Advisory 2269637, which affects how applications load external libraries. This security update addresses a particular instance of this type of vulnerability.

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CVE-2012-1854.

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

Yes. Microsoft is aware of limited, targeted attacks attempting to exploit the vulnerability.

Update Information

Detection and Deployment Tools and Guidance

Security Central

Manage the software and security updates you need to deploy to the servers, desktop, and mobile systems in your organization. For more information see the TechNet Update Management Center. The Microsoft TechNet Security website provides additional information about security in Microsoft products.

Security updates are available from Microsoft Update and Windows Update. Security updates are also available from the Microsoft Download Center. You can find them most easily by doing a keyword search for "security update."

For customers of Microsoft Office for Mac, Microsoft AutoUpdate for Mac can help keep your Microsoft software up to date. For more information about using Microsoft AutoUpdate for Mac, see Check for software updates automatically.

Finally, security updates can be downloaded from the Microsoft Update Catalog. The Microsoft Update Catalog provides a searchable catalog of content made available through Windows Update and Microsoft Update, including security updates, drivers and service packs. By searching using the security bulletin number (such as, "MS07-036"), you can add all of the applicable updates to your basket (including different languages for an update), and download to the folder of your choosing. For more information about the Microsoft Update Catalog, see the Microsoft Update Catalog FAQ.

Detection and Deployment Guidance

Microsoft provides detection and deployment guidance for security updates. This guidance contains recommendations and information that can help IT professionals understand how to use various tools for detection and deployment of security updates. For more information, see Microsoft Knowledge Base Article 961747.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) allows administrators to scan local and remote systems for missing security updates as well as common security misconfigurations. For more information about MBSA, visit Microsoft Baseline Security Analyzer.

The following table provides the MBSA detection summary for this security update.

Expand table

Software	MBSA
Microsoft Office 2003 Service Pack 3	Yes
Microsoft Office 2007 Service Pack 2 and Microsoft Office 2007 Service Pack 3	Yes
Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1 (32-bit editions)	Yes
Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1 (64-bit editions)	Yes
Microsoft Visual Basic for Applications	No

Note For customers using legacy software not supported by the latest release of MBSA, Microsoft Update, and Windows Server Update Services, please visit Microsoft Baseline Security Analyzer and reference the Legacy Product Support section on how to create comprehensive security update detection with legacy tools.

Windows Server Update Services

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. For more information about how to deploy security updates using Windows Server Update Services, see the TechNet article, Windows Server Update Services.

Systems Management Server

The following table provides the SMS detection and deployment summary for this security update.

Expand table

Software	SMS 2003 with ITMU	System Center Configuration Manager
Microsoft Office 2003 Service Pack 3	Yes	Yes
Microsoft Office 2007 Service Pack 2 and Microsoft Office 2007 Service Pack 3	Yes	Yes
Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1 (32-bit editions)	Yes	Yes
Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1 (64-bit editions)	Yes	Yes
Microsoft Visual Basic for Applications	No	No

Note Microsoft discontinued support for SMS 2.0 on April 12, 2011. For SMS 2003, Microsoft also discontinued support for the Security Update Inventory Tool (SUIT) on April 12, 2011. Customers are encouraged to upgrade to System Center Configuration Manager. For customers remaining on SMS 2003 Service Pack 3, the Inventory Tool for Microsoft Updates (ITMU) is also an option.

For SMS 2003, the SMS 2003 Inventory Tool for Microsoft Updates (ITMU) can be used by SMS to detect security updates that are offered by Microsoft Update and that are supported by Windows Server Update Services. For more information about the SMS 2003 ITMU, see SMS

2003 Inventory Tool for Microsoft Updates. For more information about SMS scanning tools, see SMS 2003 Software Update Scanning Tools. See also Downloads for Systems Management Server 2003.

System Center Configuration Manager uses WSUS 3.0 for detection of updates. For more information about System Center Configuration Manager Software Update Management, visit System Center.

For more information about SMS, visit the SMS website.

For more detailed information, see Microsoft Knowledge Base Article 910723: Summary list of monthly detection and deployment guidance articles.

Note If you have used an Administrative Installation Point (AIP) for deploying Office XP or Office 2003, you may not be able to deploy the update using SMS if you have updated the AIP from the original baseline. For more information, see the **Office Administrative Installation Point** heading in this section.

Office Administrative Installation Point

If you installed your application from a server location, the server administrator must update the server location with the administrative update and deploy that update to your system.

- For supported versions of Microsoft Office XP, see Creating an Administrative Installation Point. For more information on how to change the source for a client system from an updated administrative installation point to an Office XP original baseline source, see Microsoft Knowledge Base Article 922665.
  Note If you plan to manage software updates centrally from an updated administrative image, you can find more information in the article Updating Office XP Clients from a Patched Administrative Image.
- For supported versions of Microsoft Office 2003, see Creating an Administrative Installation Point. For more information on how to change the source for a client computer from an updated administrative installation point to an Office 2003 original baseline source or Service Pack 3 (SP3), see Microsoft Knowledge Base Article 902349.
  Note If you plan to manage software updates centrally from an updated administrative image, you can find more information in the article, Distributing Office 2003 Product Updates.

- For creating a network installation point for supported versions of Microsoft Office, see Create a network installation point for Microsoft Office.

  Note If you plan to manage security updates centrally, use Windows Server Update Services. For more information about how to deploy security updates for Microsoft Office, visit the Windows Server Update Services website.

Update Compatibility Evaluator and Application Compatibility Toolkit

Updates often write to the same files and registry settings required for your applications to run. This can trigger incompatibilities and increase the time it takes to deploy security updates. You can streamline testing and validating Windows updates against installed applications with the Update Compatibility Evaluator components included with Application Compatibility Toolkit.

The Application Compatibility Toolkit (ACT) contains the necessary tools and documentation to evaluate and mitigate application compatibility issues before deploying Windows Vista, a Windows Update, a Microsoft Security Update, or a new version of Windows Internet Explorer in your environment.

Security Update Deployment

Affected Software

For information about the specific security update for your affected software, click the appropriate link:

Office 2003 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the **Deployment Information** subsection below.

Expand table

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Deployment	

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Installing without user intervention	office2003-kb2687626-fullfile-enu.exe /q:a
Installing without restarting	office2003-kb2687626-fullfile-enu.exe /r:n
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance.** \ \ For features you can selectively install, see the **Office Features for Administrative Installations** subsection in this section.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012 .
HotPatching	Not applicable
Removal Information	This update cannot be removed.
File Information	See Microsoft Knowledge Base Article KB2687626
Registry Key Verification	Not applicable

Office Features

The following table contains the list of feature names (case sensitive) that must be reinstalled for the update. To install all features, you can use **REINSTALL=ALL** or you can install the following features:

Expand table

Product	Feature
ACCESSRT, OUTLS11, VISVEA, PPT11, ACC11, BASIC11, FP11, OUTL11, OUTLSM11, PERS11, PRO11SB, PROI11, PRO11, PUB11, STDP11, STD11, WORD11, EXCEL11, PRJPROE, PRJPRO, PRJSTDE, PRJSTD, VISPRO, VISPROR, VISSTD, VISSTDR	VBAFile

Note Administrators working in managed environments can find complete resources for deploying Office updates in an organization at the Office Admin Update Center. At that site, scroll down and look under the **Update Resources** section for the software version you are updating. The Windows Installer Documentation also provides more information about the parameters supported by Windows Installer.

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 2.0 or later version be installed on the system. All supported versions of Windows include Windows Installer 2.0 or a later version.

To install the 2.0 or later version of Windows Installer, visit one of the following Microsoft websites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Microsoft Windows 2000
- Windows Installer 2.0 Redistributable for Microsoft Windows 2000 and Windows NT 4.0

For more information about the terminology that appears in this bulletin, such as hotfix, see Microsoft Knowledge Base Article 824684.

This security update supports the following setup switches.

Supported Security Update Installation Switches

Expand table

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/q:u	Specifies user-quiet mode, which presents some dialog boxes to the user.
/q:a	Specifies administrator-quiet mode, which does not present any dialog boxes to the user.
/t:path	Specifies the target folder for extracting files.
/c	Extracts the files without installing them. If **/t:path** is not specified, you are prompted for a target folder.
/c:path	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the system after installation.
/r:l	Prompts the user to restart the system if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the system after installation.
/r:s	Restarts the system after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

Note You can combine these switches into one command. For backward compatibility, the security update also supports many of the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841.

Removing the Update

To remove this security update, use the Add or Remove Programs item in Control Panel.

Note When you remove this update, you may be prompted to insert the Microsoft Office 2003 CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs item in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**
  Because there are several editions of Microsoft Windows, the following steps may be different on your system. If they are, see your product documentation to complete these steps.

  1. Click **Start** and then enter an update file name in the **Start Search** box.
  2. When the file appears under **Programs**, right-click the file name and click **Properties**.
  3. On the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
  4. You can also click the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
  5. Finally, you can also click the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

Microsoft Office 2007 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
Deployment	
Installing without user intervention	vbe62007-kb2596744-fullfile-x86-glb.exe /passive

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
Installing without restarting	vbe62007-kb2596744-fullfile-x86-glb.exe /norestart
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance**.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012 .
HotPatching	Not applicable
Removal Information	Use **Add or Remove Programs** item in Control Panel.
File Information	See Microsoft Knowledge Base Article KB2596744
Registry Key Verification	Not applicable

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 3.1 or later version be installed on the system.

To install the 3.1 or later version of Windows Installer, visit one of the following Microsoft websites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Microsoft Windows 2000

For more information about the terminology that appears in this bulletin, such as hotfix, see Microsoft Knowledge Base Article 824684.

This security update supports the following setup switches.

Supported Security Update Installation Switches

Expand table

Switch	Description
/? or **/help**	Displays usage dialog.
/passive	Specifies passive mode. Requires no user interaction; users see basic progress dialogs but cannot cancel.
/quiet	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/norestart	Suppresses restarting the system if the update requires a restart.
/forcerestart	Automatically restarts the system after applying the update, regardless of whether the update requires the restart.
/extract	Extracts the files without installing them. You are prompted for a target folder.
/extract:<path>	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/lang:<LCID>	Forces the use of a specific language, when the update package supports that language.
/log:<log file>	Enables logging, by both Vnox and Installer, during the update installation.

Note You can combine these switches into one command. For backward compatibility, the security update also supports many of the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841.

Removing the Update

To remove this security update, use the Add or Remove Programs item in Control Panel.

Note When you remove this update, you may be prompted to insert the 2007 Microsoft Office CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs item in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771 .

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**
  Because there are several editions of Microsoft Windows, the following steps may be different on your system. If they are, see your product documentation to complete these steps.

  1. Click **Start** and then enter an update file name in the **Start Search** box.
  2. When the file appears under **Programs**, right-click the file name and click **Properties**.
  3. On the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
     Note Depending on the edition of the operating system, or the programs that are installed on your system, some files that are listed in the file information table may not be installed.
  4. You can also click the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
     Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.
  5. Finally, you can also click the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version

of the file.

Microsoft Office 2010 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
Deployment	
Installing without user intervention	For Microsoft Office 2010 (32-bit editions):\ vbe72010-kb2598243-fullfile-x86-glb.exe /passive\ ace2010-kb2553447-fullfile-x86-glb.exe /passive
For Microsoft Office 2010 (64-bit editions):\ vbe72010-kb2598243-fullfile-x64-glb.exe /passive\ ace2010-kb2553447-fullfile-x64-glb.exe /passive	
Installing without restarting	For Microsoft Office 2010 (32-bit editions):\ vbe72010-kb2598243-fullfile-x86-glb.exe /norestart\ ace2010-kb2553447-fullfile-x86-glb.exe /norestart
For Microsoft Office 2010 (64-bit editions):\ vbe72010-kb2598243-fullfile-x64-glb.exe /norestart\ ace2010-kb2553447-fullfile-x64-glb.exe /norestart	
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance**.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
	applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012.
HotPatching	Not applicable
Removal Information	Use **Add or Remove Programs** item in Control Panel.
File Information	See Microsoft Knowledge Base Article 2598243 and Microsoft Knowledge Base Article 2553447
Registry Key Verification	Not applicable

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 3.1 or later version be installed on the system.

To install the 3.1 or later version of Windows Installer, visit one of the following Microsoft websites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Microsoft Windows 2000

For more information about the terminology that appears in this bulletin, such as hotfix, see Microsoft Knowledge Base Article 824684.

This security update supports the following setup switches.

Supported Security Update Installation Switches

Expand table

Switch	Description
/? or **/help**	Displays usage dialog.
/passive	Specifies passive mode. Requires no user interaction; users see basic progress dialogs but cannot cancel.
/quiet	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/norestart	Suppresses restarting the system if the update requires a restart.
/forcerestart	Automatically restarts the system after applying the update, regardless of whether the update requires the restart.
/extract	Extracts the files without installing them. You are prompted for a target folder.
/extract:<path>	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/lang:<LCID>	Forces the use of a specific language, when the update package supports that language.
/log:<log file>	Enables logging, by both Vnox and Installer, during the update installation.

Note You can combine these switches into one command. For backward compatibility, the security update also supports many of the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841.

Removing the Update

To remove this security update, use the Add or Remove Programs item in Control Panel.

Note When you remove this update, you may be prompted to insert the 2007 Microsoft Office CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs item in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to

use the Microsoft Baseline Security Analyzer (MBSA) tool. See the section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**
  Because there are several editions of Microsoft Windows, the following steps may be different on your system. If they are, see your product documentation to complete these steps.

  1. Click **Start** and then enter an update file name in the **Start Search** box.
  2. When the file appears under **Programs**, right-click the file name and click **Properties**.
  3. On the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
     Note Depending on the edition of the operating system, or the programs that are installed on your system, some files that are listed in the file information table may not be installed.
  4. You can also click the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
     Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.
  5. Finally, you can also click the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

Microsoft Visual Basic for Applications

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**The update for this issue may be included in a future update rollup**
Deployment	
Installing without user intervention	VBA65-KB2688865-x86-ENU.exe /q:a
Installing without restarting	VBA65-KB2688865-x86-ENU.exe /r:n
Update log file	Not applicable
Further information	See the subsection, **Detection and Deployment Tools and Guidance**
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.
HotPatching	Not applicable
Removal Information	After you install the update, you cannot remove it.
File Information	See Microsoft Knowledge Base Article 2688865
Registry Key Verification	Not applicable\ \ **Note** You may be able to verify the file installed by the security update as follows:\ File version of vbe6.dll is 6.5.10.54

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system.

For more information about the terminology that appears in this bulletin, such as *hotfix*, see Microsoft Knowledge Base Article 824684 .

This security update supports the following setup switches.

Supported Security Update Installation Switches

Expand table

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/q:u	Specifies user-quiet mode, which presents some dialog boxes to the user.
/q:a	Specifies administrator-quiet mode, which does not present any dialog boxes to the user.
/t:path	Specifies the target folder for extracting files.
/c	Extracts the files without installing them. If **/t:path** is not specified, you are prompted for a target folder.
/c:path	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the system after installation.
/r:l	Prompts the user to restart the system if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the system after installation.
/r:s	Restarts the system after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

Note You can combine these switches into one command.

Removing the Update

After you install the update, you cannot remove it.

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**
  Note Because there are several versions and editions of Microsoft Windows, the following steps may be different on your system. If they are, see your product documentation to complete these steps.

1. Click **Start**, and then click **Search**.
2. In the **Search Results** pane, click **All files and folders** under **Search Companion**.
3. In the **All or part of the file name** box, type a file name from the appropriate file information table, and then click **Search**.
4. In the list of files, right-click a file name from the appropriate file information table, and then click **Properties**.
   Note Depending on the edition of the operating system, or the programs that are installed on your system, some of the files that are listed in the file information table may not be installed.
5. On the **Version** tab, determine the version of the file that is installed on your system by comparing it to the version that is documented in the appropriate file information table.
   Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.

Other Information

Acknowledgments

Microsoft thanks the following for working with us to help protect customers:

- Bai Haowen of Huawei Security Labs for reporting the Visual Basic for Applications Insecure Library Loading Vulnerability (CVE-2012-1854)

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active

protections are available from security software providers, please visit the active protections websites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners .

Support

How to obtain help and support for this security update

- Help installing updates: Support for Microsoft Update
- Security solutions for IT professionals: TechNet Security Troubleshooting and Support
- Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center
- Local support according to your country: International Support

Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (July 10, 2012): Bulletin published.
- V2.0 (November 13, 2012): Rereleased bulletin to replace the KB2598361 update with the KB2687626 update for Microsoft Office 2003 Service Pack 3 to address an issue with digital certificates described in Microsoft Security Advisory 2749655. See the update FAQ for details.

Built at 2014-04-18T13:49:36Z-07:00

Last updated on 06/08/2023