

Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

# [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0010.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 09/04/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 4 Sep 2003 11:05:44 +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>

-----

Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

---

## SUMMARY

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 make use of VBA to perform certain functions. VBA can also be used to build customized applications based around an existing host application.

A flaw exists in the way VBA checks document properties passed to it when a document is opened by the host application. A buffer overrun exists which if exploited successfully could allow an attacker to execute code of their choice in the context of the logged on user.

In order for an attack to be successful, a user would have to open a specially crafted document sent to them by an attacker. This document could be any type of document that supports VBA, such as a Word document, Excel spreadsheet, PowerPoint presentation. In the case where Microsoft Word is being used as the HTML e-mail editor for Microsoft Outlook, this document could be an e-mail, and however the user would need to reply to, or forward the mail message in order for the vulnerability to be

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

exploited.

### DETAILS

#### Affected Software:

- \* Microsoft Visual Basic for Applications SDK 5.0
- \* Microsoft Visual Basic for Applications SDK 6.0
- \* Microsoft Visual Basic for Applications SDK 6.2
- \* Microsoft Visual Basic for Applications SDK 6.3

#### Products which Include the Affected Software:

- \* Microsoft Access 97
- \* Microsoft Access 2000
- \* Microsoft Access 2002
- \* Microsoft Excel 97
- \* Microsoft Excel 2000
- \* Microsoft Excel 2002
- \* Microsoft PowerPoint 97
- \* Microsoft PowerPoint 2000
- \* Microsoft PowerPoint 2002
- \* Microsoft Project 2000
- \* Microsoft Project 2002
- \* Microsoft Publisher 2002
- \* Microsoft Visio 2000
- \* Microsoft Visio 2002
- \* Microsoft Word 97
- \* Microsoft Word 98(J)
- \* Microsoft Word 2000
- \* Microsoft Word 2002
- \* Microsoft Works Suite 2001
- \* Microsoft Works Suite 2002
- \* Microsoft Works Suite 2003
- \* Microsoft Business Solutions Great Plains 7.5
- \* Microsoft Business Solutions Dynamics 6.0
- \* Microsoft Business Solutions Dynamics 7.0
- \* Microsoft Business Solutions eEnterprise 6.0
- \* Microsoft Business Solutions eEnterprise 7.0
- \* Microsoft Business Solutions Solomon 4.5
- \* Microsoft Business Solutions Solomon 5.0
- \* Microsoft Business Solutions Solomon 5.5

#### Mitigating factors:

- \* The user must open a document sent to them by an attacker in order for this vulnerability to be exploited.
- \* When Microsoft Word is being used as the HTML e-mail editor in Outlook, a user would need to reply to or forward a malicious e-mail document sent to them in order for this vulnerability to be exploited.
- \* An attacker's code could only run with the same rights as the logged on user. The specific privileges the attacker could gain through this vulnerability would therefore depend on the privileges granted to the user. Any limitations on a user's account, such as those applied through

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

Group Policies, would also limit the actions of any arbitrary code executed by this vulnerability.

### Patch availability:

Download locations for this patch there are several versions of this patch, depending on which application you have that uses VBA. You are strongly advised to read the FAQ above entitled "There are a number of patches available for this vulnerability? Which one should I install?" in order to determine which version of the patch you should apply.

### Microsoft Office 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=E2CCE199-9C4A-4EEC-A3EC-9F738017F275&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=E2CCE199-9C4A-4EEC-A3EC-9F738017F275&displaylang=en>

### Administrative update only:

<http://www.microsoft.com/office/ork/xp/journ/o2k0901a.htm>  
<http://www.microsoft.com/office/ork/xp/journ/o2k0901a.htm>

### Microsoft Office XP (including Publisher 2002):

<http://microsoft.com/downloads/details.aspx?FamilyId=6F1FC4B0-29E9-44E0-A33D-AD6B4B6A8FF4&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=6F1FC4B0-29E9-44E0-A33D-AD6B4B6A8FF4&displaylang=en>

### Administrative update only:

<http://www.microsoft.com/office/ork/xp/journ/oxp1001a.htm>  
<http://www.microsoft.com/office/ork/xp/journ/oxp1001a.htm>

### Microsoft Project 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=E53A52E7-431D-4580-9733-B92A2B7BFD0D&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=E53A52E7-431D-4580-9733-B92A2B7BFD0D&displaylang=en>

### Microsoft Project 2002:

<http://microsoft.com/downloads/details.aspx?FamilyId=525BDE0A-0028-488A-8209-6E07D4603CCB&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=525BDE0A-0028-488A-8209-6E07D4603CCB&displaylang=en>

### Microsoft Visio 2002:

<http://microsoft.com/downloads/details.aspx?FamilyId=55944490-13C2-4043-BA2A-17AF02E9C73E&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=55944490-13C2-4043-BA2A-17AF02E9C73E&displaylang=en>

### Microsoft VBA Patch:

<http://microsoft.com/downloads/details.aspx?FamilyId=DA1A7ABA-CD3D-458B-9729-AB9094C9BD3F&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=DA1A7ABA-CD3D-458B-9729-AB9094C9BD3F&displaylang=en>

The Microsoft VBA patch can be installed on systems running the following applications:

Microsoft VBA 5.0

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

Microsoft VBA 6.0  
Microsoft VBA 6.2  
Microsoft VBA 6.3.  
Microsoft Access 97  
Microsoft Excel 97  
Microsoft PowerPoint 97  
Microsoft Word 97  
Microsoft Word 98(J)  
Microsoft Visio 2000  
Microsoft Works Suite 2001  
Microsoft Business Solutions Great Plains 7.5  
Microsoft Business Solutions Dynamics 6.0  
Microsoft Business Solutions Dynamics 7.0  
Microsoft Business Solutions eEnterprise 6.0  
Microsoft Business Solutions eEnterprise 7.0  
Microsoft Business Solutions Solomon 4.5  
Microsoft Business Solutions Solomon 5.0  
Microsoft Business Solutions Solomon 5.5

Microsoft recommends users visit Office Update at <http://www.office.microsoft.com/ProductUpdates/default.aspx> to detect and install this security patch and all other public updates to Office family products (note: Office Update does not support Office 97 or Visio 2000).

What's the scope of the vulnerability?

This is a buffer–overflow vulnerability that could allow an attacker to run arbitrary code of their choice on a user's machine in the security context of that user, if the user were to open a especially malformed document.

What causes the vulnerability?

The vulnerability results because of a flaw in the way that Microsoft Visual Basic for Applications (VBA) checks certain document properties that are passed to it from a host application when a document is opened. As a result, it is possible for the host application to pass unchecked parameters to Microsoft VBA, causing a buffer–overflow condition that could allow arbitrary code to be executed.

What is Microsoft VBA?

Microsoft VBA is a development technology for developing client desktop packaged applications and integrating them with existing data and systems. VBA is based on the Microsoft Visual Basic development system. Visual Basic for Applications provides an integrated development environment (IDE) that features the same elements familiar to developers using Microsoft Visual Basic, including a Project Window, a Properties Window, and debugging tools. Microsoft VBA also includes support for Microsoft Forms, for creating custom dialog boxes, and ActiveX® Controls, for building user interfaces. VBA is integrated directly into a host application. Software programs that include VBA are called customizable applications—applications that can be tailored to fit specific business needs.

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

Microsoft Office is one of the many applications that incorporate Microsoft VBA, allowing customers to develop custom applications based on Microsoft Office. In addition, other non-Microsoft applications incorporate Microsoft VBA.

What's wrong with Microsoft VBA?

When a document is opened by an application that supports Microsoft VBA, the host application carries out a check to determine whether Microsoft VBA is required by the document and should therefore be loaded. During an initial check some document properties are passed to Microsoft VBA – a flaw exists because Microsoft VBA does not correctly validate the data that is passed to it during this initial phase.

Does this mean that Microsoft Office does not correctly check the security on a document?

No – the flaw is in a process that is initiated before any security checks occur. The flaw is in the initial check to determine whether Microsoft VBA is required by the host application in order to handle the document being opened. As a result, any security checks such as Macro protection checks would not have occurred when the vulnerability could be encountered.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to execute code of their choice in the context of the logged on user.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by sending a user a specially crafted document designed to exploit this vulnerability, and encouraging the user to open the document. When the user opened the document, it could cause arbitrary code to execute on the system in the security context of the logged on user. In the case where Microsoft Word is being used as the e-mail editor for Microsoft Outlook – which is the default setting for Office XP – an attacker could send a specially crafted e-mail to the user, and could cause arbitrary code to be executed if the user were to reply or forward the e-mail.

An attacker could also seek to exploit this vulnerability by creating a malicious document and hosting it on a webpage, and then enticing a user to visit the website. If the user were to visit the site and follow a link to the document, the document could open automatically, and therefore could allow arbitrary code to be run.

If I'm using Microsoft Word as my e-mail editor, can the vulnerability be exploited just through reading e-mail?

No – simply reading e-mail will not allow the vulnerability to be exploited. The user must reply to or forward the attacker's e-mail.

What does the patch do?

The patch eliminates the vulnerability by ensuring that Microsoft VBA carries out the appropriate checks on the data passed to it by a host application when a document is opened.

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

There are a number of patches available for this vulnerability? Which one should I install?

This depends on which version of Microsoft VBA and which host application you are using:

Microsoft VBA Patch:

If you are using any of the following applications, you should apply the Microsoft VBA Version of the patch:

Microsoft VBA 5.0

Microsoft VBA 6.0

Microsoft VBA 6.2

Microsoft VBA 6.3.

Microsoft Access 97

Microsoft Excel 97

Microsoft PowerPoint 97

Microsoft Word 97

Microsoft Word 98(J)

Microsoft Works 2001

Microsoft Works 2002

Microsoft Works Suite 2003

Microsoft Business Solutions Great Plains 7.5

Microsoft Business Solutions Dynamics 6.0

Microsoft Business Solutions Dynamics 7.0

Microsoft Business Solutions eEnterprise 6.0

Microsoft Business Solutions eEnterprise 7.0

Microsoft Business Solutions Solomon 4.5

Microsoft Business Solutions Solomon 5.0

Microsoft Business Solutions Solomon 5.5

Microsoft Project 2000, Microsoft Project 2002 and Microsoft Visio Patches:

If you are using Microsoft Project or Microsoft Visio you should apply the specific version of the patch for those products.

Microsoft Office 2000 and Microsoft Office XP patches:

If you are using Microsoft Office 2000 or Microsoft Office XP (including Publisher 2002) you should apply the specific version of the patch for those products.

I'm using more than one of the products listed above. Should I apply the product specific patch for each product?

Yes— you should patch each product that is listed above. For example, if you are using Microsoft Office XP and Microsoft Visio 2000, you should apply both the Microsoft Office XP and Microsoft Visio versions of the patch.

How do I tell which version of Microsoft VBA I am using?

To check if VBA is present on your system and to identify which version you are running check for the following files (where C:\ is your system drive):

## Securiteam: [NT] Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution

C:\Program Files\Common Files\Microsoft Shared\VBA\vbe.dll – if this file is present you have VBA 5.0.

C:\Program Files\Common Files\Microsoft Shared\VBA\VBA6\vbe6.dll – if this file is present you have VBA 6.0.

I have a non-Microsoft application that makes use of Microsoft VBA. What should I do?

Microsoft has worked with 3rd parties who develop applications using Microsoft VBA to make sure they are aware of this security vulnerability and that they have the necessary updates to Microsoft VBA to incorporate in their products. You should contact your software vendor to obtain updates for any non-Microsoft applications that use Microsoft VBA.

### ADDITIONAL INFORMATION

The information has been provided by

<[mailto:0\\_51915\\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\\_US@Newsletters.Microsoft.com](mailto:0_51915_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com)>

Microsoft Product Security.

=====

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### 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.