

# [NT] Flaw in Microsoft Word Could Enable Macros to Run Automatically

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0007.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 09/04/03

To: list@securiteam.com

Date: 4 Sep 2003 10:20:54 +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 Microsoft Word Could Enable Macros to Run Automatically

---

## SUMMARY

A macro is a series of commands and instructions that can be grouped together as a single command to accomplish a task automatically. Microsoft Word supports the use of macros to allow the automation of commonly performed tasks. Since macros are executable code it is possible to misuse them, so Microsoft Word has a security model designed to validate whether a macro should be allowed to execute depending on the level of macro security the user has chosen.

A vulnerability exists because it is possible for an attacker to craft a malicious document that will bypass the macro security model. If the document was opened, this flaw could allow a malicious macro embedded in the document to be executed automatically, regardless of the level at which macro security is set. The malicious macro could take the same actions that the user had permissions to carry out, such as adding, changing, or deleting data or files, communicating with a web site or formatting the hard drive.

The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious document – there is no way for an attacker to

## Securiteam: [NT] Flaw in Microsoft Word Could Enable Macros to Run Automatically

force a malicious document to be opened.

### DETAILS

#### Affected Software:

- \* 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

#### Mitigating factors:

- \* The user must open the malicious document for an attacker to be successful. An attacker cannot force the document to be opened automatically.
- \* The vulnerability cannot be exploited automatically through e-mail. A user must open an attachment sent in e-mail for an e-mail borne attack to be successful.
- \* By default, Outlook 2002 block programmatic access to the Address Book. In addition, Outlook 98 and 2000 block programmatic access to the Outlook Address Book if the Outlook Email Security Update has been installed. Customers who use any of these products would not be at risk of propagating an e-mail borne attack that attempted to exploit this vulnerability.
- \* The vulnerability only affects Microsoft Word – other members of the Office product family are not affected.

#### Patch availability:

Download locations for this patch  
Microsoft Word 2002:

<http://microsoft.com/downloads/details.aspx?FamilyId=7D3775FC-F424-4B04-ABEB-9B4CA1EB182D&displayla>  
<http://microsoft.com/downloads/details.aspx?FamilyId=7D3775FC-F424-4B04-ABEB-9B4CA1EB182D&displayla>

#### Administrative update only:

<http://www.microsoft.com/office/ork/xp/journ/wrd1006a.htm>  
<http://www.microsoft.com/office/ork/xp/journ/wrd1006a.htm>

#### Microsoft Word 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=4A8F6ACE-E14E-4978-A9C9-6989CD03A4A3&displayla>  
<http://microsoft.com/downloads/details.aspx?FamilyId=4A8F6ACE-E14E-4978-A9C9-6989CD03A4A3&displayla>

#### Administrative update only:

<http://www.microsoft.com/office/ork/xp/journ/wrd0903a.htm>  
<http://www.microsoft.com/office/ork/xp/journ/wrd0903a.htm>

## Securiteam: [NT] Flaw in Microsoft Word Could Enable Macros to Run Automatically

Microsoft Word 97/Microsoft Word 98(J):

Information on receiving Microsoft Word 97 & Microsoft Word 98(J) support is available at:

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:827647>>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:827647>

Microsoft recommends users visit Office Update at

<<http://www.office.microsoft.com/ProductUpdates/default.aspx>>  
<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 vulnerability could enable an attacker to create a document that, when opened in Microsoft Word, could allow an unsigned macro to run regardless of the macro security level. Macros can take any action that the user can take, and as a result, this vulnerability could allow an attacker to take actions such as changing data, communicating with Web sites, reformatting the hard disk, or changing the Word security settings. The vulnerability only affects Word – other members of the Office product family are not affected.

What causes the vulnerability?

The vulnerability results because Word incorrectly checks properties in a modified document, causing it to not prompt the user with a macro security warning when macros are present in the document.

What's a macro?

Generally, the term macro refers to a small program that automates frequently performed tasks in an operating system or in a program. For example, all members of the Office family of products support the use of macros. This allows companies to develop macros that perform as sophisticated productivity tools that run in Word, in Excel, or in other programs.

Like any computer program, macros can be misused. Many viruses are written as macros and are embedded in Office documents. To combat this threat, Office has a security model that is designed to make sure that macros can only run when the user wants them to run. In this case, however, there is a flaw in the security model, which can be exploited when a user opens a malformed document.

What's wrong with the way Microsoft Word checks macro security?

There is a flaw in the way that Word assesses macro security when a document is opened that could allow the macro security checks to be bypassed under certain circumstances.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to create a malicious document that could allow a macro to run automatically, if an attacker persuaded a user to open the specially-crafted document. This could allow an attacker

## Securiteam: [NT] Flaw in Microsoft Word Could Enable Macros to Run Automatically

to take any action on the system that the user can take, including adding, changing, or deleting data, running other programs, or formatting the hard disk.

What could the macro do?

The macro could take any action that the user can take. This would include adding, changing, or deleting files, communicating with a Web site, reformatting the hard disk, and so forth.

A macro also could change the user's macro security level. This could include disabling macro protection. As a result, if the user were attacked by means of this vulnerability, the user's macro security level could be reduced and other macros that would otherwise be stopped by Word could be allowed to run.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by creating a specially crafted Word document that contained a malicious macro. The attacker could then send it to a user, typically through an e-mail message, and then persuade the user to open the document. An attacker could also host the specially crafted Word document on a network share or on a Web site; however, the attacker would still need to persuade the user to open the document.

Microsoft Works Suite is listed as a vulnerable product – why?

Microsoft Works Suite includes Microsoft Word. Microsoft Works users should use Office Update at:

<http://www.office.microsoft.com/ProductUpdates/default.aspx>  
<http://www.office.microsoft.com/ProductUpdates/default.aspx> to detect and to install the appropriate patch.

What does the patch do?

This patch eliminates the vulnerability by making sure that Word carries out the appropriate macro security checks when it opens a document.

### ADDITIONAL INFORMATION

The information has been provided by

[mailto:0\\_51912\\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\\_US@Newsletters.Microsoft.com](mailto:0_51912_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)

=====

=====

Securiteam: [NT] Flaw in Microsoft Word Could Enable Macros to Run Automatically

**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.