

[NT] Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run (MS03-050)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0047.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/12/03

To: list@securiteam.com

Date: 12 Nov 2003 20:29:44 +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>

Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run (MS03-050)

SUMMARY

A security vulnerability exists in Microsoft Excel that could allow malicious code execution. This vulnerability exists because of the method Excel uses to check the spreadsheet before reading the macro instructions. If successfully exploited, an attacker could craft a malicious file that could bypass the macro security model. If an affected spreadsheet was opened, this vulnerability could allow a malicious macro embedded in the file to be executed automatically, regardless of the level at which the macro security is set. The malicious macro could then 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.

A security vulnerability exists in Microsoft Word that could allow malicious code execution. This vulnerability exists due to the way Word checks the length of a data value (Macro names) embedded in a document. If a specially crafted document were to be opened it could overflow a data value in Word and allow arbitrary code to be executed. If successfully

Securiteam: [NT] Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run (MS03-050)

exploited, an attacker could then take the same actions as 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.

DETAILS

Affected Software:

* Microsoft Excel 97 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=927F8F0C-DB5A-4601-A628-2C3A1ED5D51B&dis>

Download the update

* Microsoft Excel 2000 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=9904B2A6-0CF0-4CF2-AAE0-062BDD7417D5&dis>

Download the update

* Microsoft Excel 2002 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FAB7259D-80B2-40E6-A235-581617287560&displ>

Download the update

* Microsoft Word 97 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=5261EF7F-CC89-403C-949F-5F423E68C7AF&disp>

Download the update

* Microsoft Word 98(J) –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=75B9C39D-E6BD-4CE4-BD89-6F7B5AF2BDB1&c>

Download the update

* Microsoft Word 2000 and Microsoft Works Suite 2001 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D2BD626E-401B-4FC7-BBAC-2C6B6E66D984&d>

Download the update

* Microsoft Word 2002, Microsoft Works Suite 2002, Microsoft Works Suite 2003, and * Microsoft Works Suite 2004 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=B9B4E491-0B33-423A-8FEE-27059A29B604&disp>

Download the update

Non Affected Software:

* Microsoft Office Word 2003

* Microsoft Office Excel 2003

Mitigating factors:

* If a user of Office 97 or Office 2000 has installed the Office Documentation Open Confirm Tool, the user will always get a "file open" warning dialog box when trying to open an Office document using Internet Explorer. For Office XP and Office System 2003 this "file open" warning dialog box is enabled by default.

* These vulnerabilities could only be exploited by an attacker who persuaded a user to open a malicious file – there is no way for an attacker to force a user to open a malicious file.

What is 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, many 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. 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.

What might an attacker use these vulnerabilities to do?

If successfully exploited, an attacker could cause code of their choice to run with additional privileges on the system. This could allow the attacker to add, delete or modify data on the system, or take any other action of the attacker's choice.

Who could exploit these vulnerabilities?

Any user who could entice another user to open a specially-crafted document can attempt to exploit these vulnerabilities.

How could an attacker exploit these vulnerabilities?

An attacker could seek to exploit either of these vulnerabilities by creating a specially-crafted document that contains malicious code. The attacker could then send this to a user, typically through an e-mail message, and then persuade the user to open the file. An attacker could also host the specially-crafted 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> to detect and to install the appropriate update.

CAN-2003-0821: Excel Macro Vulnerability

What's the scope of the vulnerability in Microsoft Excel?

The Excel vulnerability could enable an attacker to create a spreadsheet that, when opened, could allow an XLM (Excel 4) 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 security settings in the application.

What causes the vulnerability in Microsoft Excel?

This vulnerability exists because of the method Excel uses to check the spreadsheet before reading the macro instructions. As a result the user will not be prompted with a macro security warning even when macros are present in the file.

What's wrong with the way Excel handles macro security?

Because of the way Excel reads and assesses macro security when a file is opened, under certain circumstances, macro security checks could be bypassed.

What does the update for Microsoft Excel do?

The update addresses the vulnerability by modifying the way that Excel performs macro security checks before opening a file.

CAN-2003-0820: Word Buffer Overrun Vulnerability

What's the scope of the vulnerability in Microsoft Word?

The Word buffer overrun vulnerability could enable an attacker to create a word document containing a Macro that, if successfully exploited, could allow an attacker to then take the same actions as 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.

What causes the vulnerability in Microsoft Word?

The vulnerability is the result of the way Word validates of the length of a data value (Macro names) embedded in a document. If successfully exploited an attacker could then take the same actions as 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.

What's wrong with the way Word handles input buffers?

Because of the way Word validates the length of an input buffer, under certain circumstances, this validation could lead to a buffer overrun.

What does the update for Microsoft Word do?

The update corrects the buffer overrun by properly validating the input buffer before opening a file.

ADDITIONAL INFORMATION

The information has been provided by 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

In order to subscribe to the mailing list, simply forward this email to: 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.