

[NT] Microsoft Excel/PowerPoint Documents can Bypass Microsoft Macro Security Checking

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0029.html>

From: support@securiteam.com

Date: 10/09/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Microsoft Excel/PowerPoint Documents can Bypass Microsoft Macro Security Checking

Message-Id: <20011009193955.57B4F138C4@mail.der-keiler.de>

Date: Tue, 9 Oct 2001 21:39:55 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Microsoft Excel/PowerPoint Documents can Bypass Microsoft Macro Security Checking

SUMMARY

Microsoft Office applications versions 2000 and later have three security settings for macro running. The "Low" setting allows all macros to run. Setting the security to "Medium" displays a warning window stating the dangers of opening documents containing Macros. This pop-up allows the user to make the decision whether to enable or disable the macro. Under the "High" setting, unsigned macros are disabled automatically. Microsoft Office applications prior to the 2000 version had much simpler macro security models.

Symantec engineers have discovered that by specifically modifying the data stream in a document file containing a macro, the Microsoft Office security settings for macros are completely bypassed in all versions of Microsoft PowerPoint and Excel products.

This issue was initially reported to Microsoft Security on 26 June 2001.

DETAILS

Securiteam: [NT] Microsoft Excel/PowerPoint Documents can Bypass

Affected Components:

- * Microsoft Excel 97 for Windows
- * Microsoft Excel 98 for Windows
- * Microsoft Excel 2000 for Windows
- * Microsoft Excel 2001 for Macintosh
- * Microsoft Excel 2002 for Windows
- * Microsoft PowerPoint 97 for Windows
- * Microsoft PowerPoint 98 for Windows
- * Microsoft PowerPoint 2000 for Windows
- * Microsoft PowerPoint 2001 for Macintosh
- * Microsoft PowerPoint 2002 for Windows

All versions of these individual products bundled in Microsoft Office Suites Microsoft Excel 98 and PowerPoint 98 for Macintosh, although not tested by Symantec, should be considered vulnerable to this issue as well.

Impact:

Unauthorized macro files, potentially containing malicious code, can run without warning, successfully bypassing Microsoft's security features. Attacker could run arbitrary code with user privileges.

Details:

Symantec engineers discovered a bug in the way macros are loaded in all versions of Microsoft PowerPoint and Excel. Under normal circumstances, with high or medium security setting enabled, whenever a Microsoft PowerPoint or Excel document is received it is scanned for macros. If the document contains a macro, a security-warning prompt is displayed under medium security. Alternatively, if the macro is recognized as un-trusted, it is disabled under the high security setting. Microsoft Office versions prior to 2000 provided a much simpler security model. By specifically modifying the data stream in the document file, the Microsoft security scanner is prevented from recognizing an embedded macro, resulting in its execution when the document is opened. Exploiting this vulnerability in susceptible Microsoft products enables an attacker to construct potentially malicious macro code to automatically run when such a modified document is opened on a target machine.

The malicious macro is able to take any action with privileges of the user on the targeted system.

This has been successfully tested in PowerPoint and Excel 97 SR-2, PowerPoint and Excel 98, PowerPoint and Excel 2000, and PowerPoint and Excel 2002 as well as PowerPoint and Excel 2001 for Macintosh. Under PowerPoint 2002, the version included in Microsoft Office XP, even unsigned macros can be executed at the highest security settings (the Run option is not disabled).

NOTE: A similar exploit exists for Microsoft Word, however the Microsoft Security patch available in Microsoft Security Bulletin MS01-034 for Steven McLeod's Microsoft Word macro exploit also protects against this exploit. Symantec urges all Microsoft Word users, who have not applied the patch in MS01-34, immediately download, and apply that patch as well for maximum protection.

Securiteam: [NT] Microsoft Excel/PowerPoint Documents can Bypass

Security response:

Symantec highly recommends all users ensure they are running a current AV product with the latest updates and script blocking to protect against unauthorized executables and other hostile code running on the user's system. Microsoft application users should ensure that all security patches are up-to-date.

Additionally, Microsoft has released a security bulletin, MS01-050, for this issue with links to product security patches. Users of individual Microsoft Office products as well as bundled Microsoft Office suites should download and install the appropriate security patches to secure their applications:

NOTE: Microsoft no longer supports Microsoft Excel or PowerPoint 97/98 versions. Symantec strongly suggests that all users of these vulnerable versions upgrade as soon as possible to a supported version and apply all appropriate security patches.

Patch availability:

Download locations for this patch

* Microsoft Excel 2000 for Windows:

<http://download.microsoft.com/download/excel2000/e2kmac/1/w98nt42kme/en-us/e2kmac.exe>
<http://download.microsoft.com/download/excel2000/e2kmac/1/w98nt42kme/en-us/e2kmac.exe>

* Microsoft Excel 2002 for Windows:

<http://download.microsoft.com/download/excel2002/exc1001/1/w98nt42kme/en-us/exc1001.exe>
<http://download.microsoft.com/download/excel2002/exc1001/1/w98nt42kme/en-us/exc1001.exe>

* Microsoft Excel 98 for Macintosh:

<http://www.microsoft.com/mac/download/office98/pptxlmacro.asp>
<http://www.microsoft.com/mac/download/office98/pptxlmacro.asp>

* Microsoft Excel 2001 for Macintosh:

<http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp>
<http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp>

* Microsoft PowerPoint 2000 for Windows:

<http://download.microsoft.com/download/powerpoint2000/p2kmac/1/w98nt42kme/en-us/p2kmac.exe>
<http://download.microsoft.com/download/powerpoint2000/p2kmac/1/w98nt42kme/en-us/p2kmac.exe>

* Microsoft PowerPoint 2002 for Windows:

<http://download.microsoft.com/download/powerpoint2002/ppt1001/1/w98nt42kme/en-us/ppt1001.exe>
<http://download.microsoft.com/download/powerpoint2002/ppt1001/1/w98nt42kme/en-us/ppt1001.exe>

* Microsoft PowerPoint 98 for Macintosh:

<http://www.microsoft.com/mac/download/office98/pptxlmacro.asp>
<http://www.microsoft.com/mac/download/office98/pptxlmacro.asp>

* Microsoft PowerPoint 2001 for Macintosh:

<http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp>
<http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp>

What's the scope of the vulnerability?

This vulnerability could enable a malicious user to create specially

Securiteam: [NT] Microsoft Excel/PowerPoint Documents can Bypass

formed Excel or PowerPoint files that would bypass macro security and execute automatically when the document is opened. Because macros by design can take any action that the user is able to take, this vulnerability could allow an attacker to take actions such as changing or deleting data, communicating with web sites, or changing the macro security settings.

This would not be able to take any actions that the user is not normally capable of. As such, access controls that limit the user's abilities would also limit the ability of the malicious documents. Further, a successful attack would require that the user open the malicious document. Best practices recommend that users not open documents from unknown or untrusted sources.

What causes the vulnerability?

The vulnerability results because the macro-detecting framework can fail to detect all instances in which the macro processor can execute macro commands. When a valid document is intentionally designed to obfuscate the presence of macros, it is still possible for those macros to execute.

What are macros?

Macros are small programs within applications such as Excel and PowerPoint. When macros run, they can take actions within the application or the operating system as if they were the user. An example of a simple action a macro might take in an application would be to find and replace text within a document. A more sophisticated macro might include features that perform automatic formatting on a document, copy files from the local system to the network, and send review copies by email.

Because macros are small programs, it is possible for attackers to create malicious macros that take undesirable actions, such as deleting files, sending unwanted messages by email, or changing the data in documents. To help protect against malicious macros, Excel and PowerPoint have a security model that prevent macros from executing without warning.

What's wrong with the macro protection in Excel and PowerPoint?

It is possible for a malicious user to create an especially malformed Excel or PowerPoint document that would bypass the macro protections and allow macros to execute automatically.

Is it possible to create a document like this by accident?

No. It is not possible to create a document that bypasses macro protection by accident. It would require very specific, detailed knowledge and such a document would have to be specifically constructed with malicious intent.

What could an attacker use this vulnerability to do?

This could allow an attacker to construct a malicious document with macro code that would run automatically when the user opened the document.

What actions could the malicious document take?

Because macros take action on behalf of the user, a macro virus that ran

Securiteam: [NT] Microsoft Excel/PowerPoint Documents can Bypass

would be able to take actions that the user himself is able to take, including changing or deleting files, sending data to external web sites, or reformatting the hard drive.

It is important to highlight that this means that it is possible for a macro virus to reset the user's security settings. A successful macro virus attack could leave a system vulnerable to future attack by disabling the security settings.

How would an attacker carry out an attack against this vulnerability?
An attacker could carry out an attack by several different routes. She could host a malicious document on a web site internally or on the Internet. She could place a malicious document on any file server to which she had appropriate permissions. Additionally, she could target specific individuals by sending a copy through email.

It's important to note that all attempts to carry out an attack require the potential victim to open the document. It is not possible to exploit this vulnerability without the user's action. Opening documents only from known, trusted sources will help to protect against an attempt to maliciously exploit this vulnerability.

What does the patch do?

The patch eliminates the vulnerability by improving the code that detects the presence of macros in these document types.

Who should apply the patch?

Anyone using or administering systems running the affected software versions should apply the patch

I am running Excel 97 and/or PowerPoint 97, does this issue affect me?

First, it is important to understand that Excel and PowerPoint 97 do not have the same macro security framework as Excel and PowerPoint 2000 and 2002. The Excel and PowerPoint 97 macro security framework lacks many key features that the 2000 and 2002 macro security framework has, including a digital signature trust model that allows trusted, signed macros to be differentiated from untrusted, unsigned macros. Under this older framework, it is difficult for a user to make an informed decision regarding the trustworthiness of macros.

In addition, as noted under "Tested Versions", Excel and PowerPoint 97 are no longer supported products.

Because of these two issues, customers who are concerned about macro security are urged to upgrade to a support version with a more robust macro security model.

Are other members of the Office Suite vulnerable?

No. All members of the Office Suites for Windows and Macintosh were tested. No other products in the Office Suite were found to be vulnerable.

Securiteam: [NT] Microsoft Excel/PowerPoint Documents can Bypass

ADDITIONAL INFORMATION

The information has been provided by <mailto:symsecurity@symantec.com>
Sym Security and <mailto:secnotif@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

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.

-
- **Previous message:** support@securiteam.com: "[\[UNIX\] OpenBSD Bug Allows Unprivileged Users to Send SIGURG and SIGIO Signals](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)