

# [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00038.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 15 Feb 2007 10:59:09 +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>

-----

Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

---

## SUMMARY

This update resolves two newly discovered, privately and publicly reported vulnerabilities in Microsoft Office.

## DETAILS

### Affected Software:

- \* Microsoft Office 2000 Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>

Download the update (KB 929062)

- \* Microsoft Access 2000

- \* Microsoft Excel 2000

- \* Microsoft FrontPage 2000

- \* Microsoft Outlook 2000

- \* Microsoft PowerPoint 2000

- \* Microsoft Publisher 2000

- \* Microsoft Word 2000

- \* Microsoft Office XP Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>

Download the update (KB926063)

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

- \* Microsoft Access 2002
- \* Microsoft Excel 2002
- \* Microsoft FrontPage 2002
- \* Microsoft Outlook 2002
- \* Microsoft PowerPoint 2002
- \* Microsoft Publisher 2002
- \* Microsoft Visio 2002
- \* Microsoft Word 2002
- \* Microsoft Office 2003 Service Pack 2 –  
<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>  
Download the update (KB929064)
- \* Microsoft Access 2003
- \* Microsoft Excel 2003
- \* Microsoft Excel 2003 Viewer
- \* Microsoft FrontPage 2003
- \* Microsoft InfoPath 2003
- \* Microsoft OneNote 2003
- \* Microsoft Outlook 2003
- \* Microsoft PowerPoint 2003
- \* Microsoft Project 2003
- \* Microsoft Publisher 2003
- \* Microsoft Visio 2003
- \* Microsoft Word 2003
- \* Microsoft Excel 2003 Viewer
- \* Microsoft Word 2003 Viewer
- \* Microsoft Project 2000 Service Release 1 –  
<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>  
Download the update (KB929062)
- \* Microsoft Project 2002 Service Pack 1 –  
<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>  
Download the update (KB929063)
- \* Microsoft Visio 2002 Service Pack 2 –  
<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>  
Download the update (KB929063)
- \* Microsoft Office 2004 for Mac –  
<<http://www.microsoft.com/downloads/details.aspx?familyid=20E089E7-7DD3-44A4-ABFE-6D8C27721683>>  
Download the update (KB932185)

### Non-Affected Software:

- \* 2007 Microsoft Office System
- \* Microsoft Office 2003 Service Pack 2
- \* Microsoft PowerPoint 2003 Viewer
- \* Microsoft Works Suites:
  - \* Microsoft Works Suite 2004
  - \* Microsoft Works Suite 2005
  - \* Microsoft Works Suite 2006

### PowerPoint Malformed Record Memory Corruption Vulnerability – CVE-2006-3877:

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opened a specially crafted file. Such a file

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

### Mitigating Factors for PowerPoint Malformed Record Memory Corruption Vulnerability – CVE-2006-3877:

- \* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.

- \* In a Web-based attack scenario, an attacker would have to host a Web site that contains a PowerPoint file that is used to attempt to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

- \* The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.

- \* Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and Office 2003.

- \* 2007 Microsoft Office System is not affected by this vulnerability.

- \* PowerPoint 2003 Viewer is not affected by this vulnerability.

### Workarounds for PowerPoint Malformed Record Memory Corruption Vulnerability – CVE-2006-3877:

- \* Do not open or save Microsoft PowerPoint files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

### FAQ for PowerPoint Malformed Record Memory Corruption Vulnerability – CVE-2006-3877:

What is the scope of the vulnerability?

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opens a file containing malformed record. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

What causes the vulnerability?

The vulnerability is caused when PowerPoint opens a specially crafted PowerPoint file which will result in the access of memory outside intended regions when parsing placeholder data.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opened the file.

How could an attacker exploit the vulnerability?

In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or instant messenger message that takes users to the attacker's Web site.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and by persuading the user to open the file.

What systems are primarily at risk from the vulnerability?

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 removes the vulnerability by modifying the way that PowerPoint parses the file and validates the record before passing it to the allocated buffer.

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

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued. This security bulletin addresses the privately disclosed vulnerability as well as additional issues discovered through internal investigations.

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

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

### Excel Malformed Record Vulnerability – CVE-2007-0671:

A remote code execution vulnerability exists in Excel and could be exploited when Excel opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

### Mitigating Factors for Excel Malformed Record Vulnerability – CVE-2007-0671:

\* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.

\* In a Web-based attack scenario, an attacker would have to host a Web site that contains an Excel file that is used to attempt to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

\* The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.

\* Users who have installed and are using the

<http://www.microsoft.com/downloads/details.aspx?familyid=8B5762D2-077F-4031-9EE6-C9538E9F2A2F>> Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and Office 2003.

\* 2007 Microsoft Office System is not affected by this vulnerability.

Workarounds for Excel Malformed Record Vulnerability – CVE-2007-0671:

\* Do not open or save Microsoft Excel files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Excel Malformed Record Vulnerability – CVE-2007-0671:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in Excel and could be exploited when Excel opens a file containing malformed record. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user were 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

What causes the vulnerability?

The vulnerability is caused when Excel opens a specially crafted Excel file which will result in the access of memory outside intended regions when parsing placeholder data.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opened the file.

How could an attacker exploit the vulnerability?

In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or instant messenger message that takes users to the attacker's Web site.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted Excel file to the user and by persuading the user to open the file.

[NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS07-015)

What systems are primarily at risk from the vulnerability?

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 removes the vulnerability by modifying the way that Excel parses the file and validates the record before passing it to the allocated buffer.

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-2007-0671.

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

Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-015.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-015.msp>>  
<http://www.microsoft.com/technet/security/bulletin/ms07-015.msp>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

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.