

# [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS08-016)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00043.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 16 Mar 2008 11:49:32 +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 (MS08-016)

---

## SUMMARY

This security update resolves two privately reported vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a malformed Office file. 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 impacted than users who operate with administrative user rights.

This security update is rated Critical for supported editions of Microsoft Office 2000 and rated Important for supported editions of Microsoft Office XP, Microsoft Office 2003 Service Pack 2, Microsoft Excel Viewer 2003 and Microsoft Excel Viewer 2003 Service Pack 3, and Microsoft Office 2004 for Mac. For more information, see the subsection, Affected and Non-Affected Software, in this section.

## DETAILS

Affected Software:

## [NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS08-016)

Office Suite and Other Software – Maximum Security Impact – Aggregate  
Severity Rating – Bulletins Replaced by this Update

\*

<<http://www.microsoft.com/downloads/details.aspx?familyid=72735aa1-e22c-40ed-8c79-38fba89979aa>>  
Microsoft Office 2000 Service Pack 3 (KB947361) – Remote Code Execution – Critical – MS07-025

\*

<<http://www.microsoft.com/downloads/details.aspx?familyid=9cf8aafa-71a5-4017-b53c-4e80ef6e1188>>  
Microsoft Office XP Service Pack 3 (KB947866) – Remote Code Execution – Important – MS07-025

\*

<<http://www.microsoft.com/downloads/details.aspx?familyid=9f25922c-d3c2-4ef1-b164-8a21a77d29aa>>  
Microsoft Office 2003 Service Pack 2 (KB947355) – Remote Code Execution – Important – None

\*

<<http://www.microsoft.com/downloads/details.aspx?familyid=9f25922c-d3c2-4ef1-b164-8a21a77d29aa>>  
Microsoft Office Excel Viewer 2003 (KB947355) and  
<<http://www.microsoft.com/downloads/details.aspx?familyid=9f25922c-d3c2-4ef1-b164-8a21a77d29aa>>  
Microsoft Office Excel Viewer 2003 Service Pack 3 (KB947355) – Remote Code Execution – Important – None

\*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=95DCEB37-B35F-46DB-B280-DB0F3B298AA9>>  
Microsoft Office 2004 for Mac (KB949357) – Remote Code Execution – Important – MS08-013

Non-Affected Software:

- \* Microsoft Office 2003 Service Pack 3
- \* Microsoft PowerPoint Viewer 2003
- \* Microsoft Visio 2002 Service Pack 2
- \* Microsoft Visio 2003 Viewer
- \* Microsoft Word Viewer 2003
- \* Microsoft Project 2000 Service Pack 1
- \* Microsoft Project 2002 Service Pack 2
- \* 2007 Microsoft Office System
- \* 2007 Microsoft Office System Service Pack 1
- \* Microsoft Office 2008 for Mac

Microsoft Office Cell Parsing Memory Corruption Vulnerability –  
CVE-2008-0113

A remote code execution vulnerability exists in the way Microsoft Office handles specially crafted Excel files. An attacker could exploit the vulnerability by creating a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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.

[NT] Vulnerabilities in Microsoft Office Allows Code Execution (MS08-016)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0113>>  
CVE-2008-0113

Microsoft Office Memory Corruption Vulnerability – CVE-2008-0118

A remote code execution vulnerability exists in the way Microsoft Office processes malformed Office files. An attacker could exploit the vulnerability by creating a malformed Office file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0118>>  
CVE-2008-0118

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS08-016.msp>>  
<http://www.microsoft.com/technet/security/bulletin/MS08-016.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@xxxxxxxxxxxxxxxxx

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

=====

=====

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.