

[NT] Vulnerability in Microsoft Excel Allows Remote Code Execution (MS04-033)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0038.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 15:34:51 +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 Excel Allows Remote Code Execution (MS04-033)

SUMMARY

A remote code execution vulnerability exists in Microsoft Excel. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

DETAILS

Vulnerable Systems:

* Microsoft Office 2000 Software Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B0C40C24-4DDE-45AF-8433-6DBDDD030C30>>
Download the update (KB873372)

* Microsoft Office XP Software Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5E0FADD3-1554-4C43-9B4A-D5E031478892>>
Download the update (KB873366)

* Microsoft Office 2001 for Mac –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9889BEAE-4771-415D-8070-3E51F4CC7AE3>>

Securiteam: [NT] Vulnerability in Microsoft Excel Allows Remote Code Execution (MS04-033)

Download the update

* Microsoft Office v. X for Mac –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=148E9283-4DF8-4A75-9671-CC72E6306B84>>

Download the update

Immune Systems:

* Microsoft Office XP Service Pack 3

* Microsoft Office Excel 2003

* Microsoft Office 2003 Service Pack 1

* Microsoft Excel 2004 for Mac

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0846>>

CAN-2004-0846

A remote code execution vulnerability exists in Excel. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system.

Mitigating Factors for Excel Vulnerability

* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to 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. At this point a user could be exploited.

* An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

* Excel 2001 for Mac users and Excel v. X for Mac users are prompted to download an Excel file before they open it. Therefore, a user may not be exploited by an attacker upon an initial visit to a web site.

* Office XP Service Pack 3 is not affected by this vulnerability.

* Office 2003 and Office 2003 Service Pack 1 are not affected by this vulnerability.

* Excel 2004 for Mac is not affected by this vulnerability.

FAQ for Excel Vulnerability

What is the scope of the vulnerability ?

This is a remote code execution vulnerability. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

Securiteam: [NT] Vulnerability in Microsoft Excel Allows Remote Code Execution (MS04-033)

How could an attacker exploit the vulnerability ?

An attacker could host a malicious Excel file on a web site and persuade a user to click a link to the file. The file could then be executed allowing the attacker to execute code of their choice. An attacker could also attempt to exploit the vulnerability by sending a specially crafted file in email.

What systems are primarily at risk from the vulnerability ?

Workstations and terminal servers are primarily at risk. Servers are only at risk if users who do not have sufficient administrative credentials are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Are all versions of Office and Excel affected by this vulnerability ?

No. Office XP Service Pack 3, Office 2003 and Excel 2003, Office 2003 Service Pack 1, and Excel 2004 for Mac are not affected.

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

No. Microsoft received information about this vulnerability through responsible disclosure.

What does the update do ?

The patch removes the vulnerability by making sure that Excel correctly validates parameters when it opens an Excel file.

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/MS04-033.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS04-033.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@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.