

[NT] Microsoft Excel Formula Size and Column Index Vulnerabilities (MS06-012)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00056.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Mar 2006 12:28:26 +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>

Microsoft Excel Formula Size and Column Index Vulnerabilities (MS06-012)

SUMMARY

<<http://office.microsoft.com/en-us/FX010858001033.aspx>> Microsoft Excel is a popular spreadsheet program of Microsoft Office product.

Column Index Improper Memory Access and Excel Formula Size Stack Overflow vulnerabilities have been discovered in the Microsoft Excel software.

DETAILS

Microsoft Excel Formula Size Stack Overflow:

This vulnerability is due to Microsoft Excel's manipulation of opcode 0x0218, when provided with a large Formula Size, it will cause a stack overflow.

An remote attacker could construct a .xls file and put it on controlled web site. When the user opens the .xls file with Microsoft Internet Explorer, the browser will call Microsoft Excel to open the .xls file automatically, and this will cause Microsoft Excel to crash.

If an excel file is specially crafted, it may allow attackers to execute

[NT] Microsoft Excel Formula Size and Column Index Vulnerabilities (MS06-012)

arbitrary code on the affected system.

Microsoft Excel Column Index Improper Memory Access:

This vulnerability is due to Microsoft Excel's manipulation of opcode 0x001D, when provided with a random Column Index, it will cause a Improper Memory Access.

An remote attacker could construct a .xls file and put it on controlled web site. When the user opens the .xls file with Microsoft Internet Explorer, the browser will call Microsoft Excel to open the .xls file automatically, and this will cause Microsoft Excel to crash.

If excel file is specially crafted, it may allow attackers to execute arbitrary code on the affected system.

Solution:

Microsoft has released a update for this vulnerability, which is available for downloading from Microsoft web site.

ADDITIONAL INFORMATION

The original articles could be found at:

- <<http://www.fortinet.com/FortiGuardCenter/FSA-2006-08.html>>
- <http://www.fortinet.com/FortiGuardCenter/FSA-2006-08.html>
- <<http://www.fortinet.com/FortiGuardCenter/FSA-2006-09.html>>
- <http://www.fortinet.com/FortiGuardCenter/FSA-2006-09.html>

Related articles could be found at:

- <<http://www.microsoft.com/technet/security/Bulletin/MS06-012.mspx>>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-012.mspx>
- <<http://www.securiteam.com/windowsntfocus/5TP0B1FI0C.html>>
- <http://www.securiteam.com/windowsntfocus/5TP0B1FI0C.html>

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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.