

[NT] Microsoft Excel DVAL Heap Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00025.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Mar 2008 09:37:44 +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 DVAL Heap Corruption Vulnerability

SUMMARY

<<http://office.microsoft.com/excel/>> Microsoft Excel is "the spreadsheet application that is included with Microsoft Corp's Office productivity software suite". Remote exploitation of a heap corruption vulnerability in Microsoft Corp.'s Excel spreadsheet application allows attackers to execute arbitrary code in the context of the user who started Excel.

DETAILS

Vulnerable Systems:

- * Microsoft Excel 2003
- * Microsoft Excel 2007

The vulnerability exists in the handling of DVAL records in BIFF8 format spreadsheet files. When certain fields are set to invalid values, heap corruption occurs.

Analysis:

Exploitation allows attackers to execute arbitrary code in the context of the user who started Excel. Exploitation requires that attackers persuade

[NT] Microsoft Excel DVAL Heap Corruption Vulnerability

users to open a maliciously crafted file in Excel.

Workaround:

Disabling support for legacy binary file formats in the registry will prevent exploitation of this issue. However, this workaround is not available for all versions of Microsoft Excel.

Vendor response:

Microsoft has officially addressed this vulnerability with Security Bulletin MS08-014. Previous releases, specifically Office 2007 SP1 and Office 2003 SP3, included a fix for this issue. For more information, consult their bulletin at the following URL:

<<http://www.microsoft.com/technet/security/Bulletin/ms08-014.msp>>
<http://www.microsoft.com/technet/security/Bulletin/ms08-014.msp>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0111>>
CVE-2008-0111

Disclosure Timeline:

- 05/09/2007 – Initial vendor notification
- 05/09/2007 – Initial vendor response
- 03/11/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=671>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=671>

=====

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.