

[NT] Microsoft Excel Rich Text Memory Corruption Vulnerability (MS08-014)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00051.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 16 Mar 2008 14:49:00 +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 Rich Text Memory Corruption Vulnerability (MS08-014)

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Office Excel. Exploitation requires that the attacker coerce the target into opening a malicious .XLS file.

DETAILS

Vulnerable Systems:

- * Microsoft Office Excel 2003
- * Microsoft Office Excel 2002
- * Microsoft Office Excel 2000

The specific flaw exists within the parsing of the BIFF file format used by Microsoft Excel. During the processing of a malformed tag a heap allocation can be adversely controlled. When user supplied data is copied to a heap buffer the resulting data results in a arbitrary memory overwrite. If successfully exploited this could lead to system compromise under the credentials of the currently logged in user.

Vendor Response:

[NT] Microsoft Excel Rich Text Memory Corruption Vulnerability (MS08-014)

Microsoft has issued an update to correct this vulnerability. More details can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS08-014.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS08-014.msp>

Disclosure Timeline:

2007-10-17 – Vulnerability reported to vendor
2008-03-11 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0116>>
CVE-2008-0116

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dvlabs@xxxxxxxxxxxxxxxx>>
TippingPoint DV Labs.
The original article can be found at:
<<http://dvlabs.tippingpoint.com/advisory/TPTI-08-03>>
<http://dvlabs.tippingpoint.com/advisory/TPTI-08-03>

=====

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.