

[VulnWatch] NSFOCUS SA2006-05 : Microsoft Excel SELECTION Record Memory Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-07/msg00005.html>

- *From:* NSFOCUS Security Team <security@xxxxxxxxxxx>
 - *Date:* Wed, 12 Jul 2006 15:43:28 +0800
-

NSFOCUS Security Advisory (SA2006-05)

Microsoft Excel SELECTION Record Memory Corruption Vulnerability

Release Date: 2006-07-12

CVE ID: CVE-2006-1302

<http://www.nsfocus.com/english/homepage/research/0605.htm>

Affected systems & software

=====

Microsoft Excel 2000

Microsoft Excel 2002

Microsoft Excel 2003

Unaffected systems & software

=====

Summary

=====

NSFocus Security Team discovered a memory corruption vulnerability in Microsoft Excel's processing of SELECTION record, which allows remote attackers to run arbitrary via carefully crafted Excel files.

Description

=====

Excel does not perform sufficient check for certain field when processing SELECTION record. During some data copying operation the user-supplied data might be used for the copying, resulting in memory corruption and arbitrary code execution.

Attackers can craft an Excel file with malformed SELECTION record and allure

[VulnWatch] NSFOCUS SA2006-05 : Microsoft Excel SELECTION Record Memory Corruption Vulnerability

users to open it via instant messaging tools, e-mail or other vectors, resulting in arbitrary code execution with the privilege of the user. If the user is the administrator, then attackers might take complete control over the system.

Workaround

=====

Do not open any Excel file from untrusted sources.

Vendor Status

=====

2006.03.30 Informed the vendor

2006.04.03 Vendor confirmed the vulnerability

2006.07.11 Microsoft has released a security bulletin (MS06-037) and related patches.

For more details about the security bulletin, please refer to:

<http://www.microsoft.com/technet/security/bulletin/MS06-037.mspx>

Additional Information

=====

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2006-1302 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems. Candidates may change significantly before they become official CVE entries.

Acknowledgment

=====

Wen Yujie of NSFocus Security Team found the vulnerability.

DISCLAIMS

=====

THE INFORMATION PROVIDED IS RELEASED BY NSFOCUS "AS IS" WITHOUT WARRANTY OF ANY KIND. NSFOCUS DISCLAIMS ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, EXCEPT FOR THE WARRANTIES OF MERCHANTABILITY. IN NO EVENT SHALL NSFOCUS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF NSFOCUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. DISTRIBUTION OR REPRODUCTION OF THE INFORMATION IS PROVIDED THAT THE ADVISORY IS NOT MODIFIED IN ANY WAY.

Copyright 1999-2006 NSFOCUS. All Rights Reserved. Terms of use.

NSFOCUS Security Team <security@xxxxxxxxxxx>
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD
(<http://www.nsfocus.com>)

[VulnWatch] NSFOCUS SA2006-05 : Microsoft Excel SELECTION Record Memory Corruption Vulnerability

PGP Key: <http://www.nsfocus.com/homepage/research/pgpkey.asc>

Key fingerprint = F8F2 F5D1 EF74 E08C 02FE 1B90 D7BF 7877 C6A6 F6DA