

[NT] Microsoft Excel Length Parameter Parsing Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0060.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/18/04

To: list@securiteam.com

Date: 18 Oct 2004 09:46:20 +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 Length Parameter Parsing Buffer Overflow Vulnerability

SUMMARY

An unvalidated length value used by Excel to read a string will trigger a buffer overflow on the affected system, when opening a malicious file.

DETAILS

Vulnerable Systems:

- * Microsoft Office 2000 Service Pack 3 Software (Excel 2000)
- * Microsoft Office XP Software (Excel 2002)
- * Microsoft Office 2001 for Mac (Excel 2001 for Mac)
- * Microsoft Office v. X for Mac (Excel v. X for Mac)

Microsoft Excel will read a value from an excel file and use this as the 'length' parameter when copying a string. By setting this to a large value, it is possible to cause a stack overflow leading to the control of EIP and other important registers.

Attempted exploitation will result in an event log entry similar to:

Application popup:

EXCEL.EXE – Application Error : The exception Privileged instruction.

Securiteam: [NT] Microsoft Excel Length Parameter Parsing Buffer Overflow Vulnerability

(0xc0000096) occurred in the application at location 0x#####.

Remote exploitation through Internet Explorer can be obtained through the use of an iframe or other similar object to open a file from a public UNC share or through a 'coupled' browser exploit that saves the file to a known location before opening it. Internet Explorer will automatically open the corrupt excel spreadsheet, leading to exploitation.

Vendor Status:

Microsoft has released a fix for this vulnerability in one of their latest security advisories. The advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/6T00D0UBFK.html>>

<http://www.securiteam.com/windowsntfocus/6T00D0UBFK.html>

The original Microsoft advisory can be found at

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

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

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:brett.moore@security-assessment.com>> Brett Moore.

=====

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.