

Microsoft Excel File Embedded Shockwave Flash Object Bug

20th Jun, 2006

CVE ID - CVE-2006-3014

MSRC ID – 6542sd

I. DESCRIPTION

Malicious Flash files with explicit java scripts can be embedded within excel spreadsheets using a “Shockwave Flash Object” which can be made to run once the file is opened by the user. It doesn't require user's intervention to activate the object rather it runs automatically once the file is opened.

An attacker can use excel as a container to spread malicious flash files which will execute once the excel file is opened by the user. For more details refer the PoC below.

Note: The same flash file does not directly run when it is *inserted* into the excel file as *objects*. However if it is embedded using "Shockwave Flash Object", it plays *on load* of the excel file. Here there is no user intervention required to trigger the flash file. It automatically plays once the excel file is opened.

II. TESTING ENVIRONMENT

This test has been performed on –

Windows 2003 (SP1)

Windows XP Professional Edition (SP1 / SP2) + Office 2003

Windows 2000 Professional + Office 2003

III. PROOF-OF-CONCEPT

To reproduce the exploit follow the steps below –

- Compile the flash file (“.swf”) with the malicious javascript as payload. Flash action scripts like “GetURL” can be used in order to execute any javascript or direct the victim to any malicious sites. For Example, the javascript can be invoked in the following manner:

```
getURL("javascript:window.open('http://www.google.com', 'Tr0y', config='height=300,width=300');");
```

```
getURL("javascript:document.write('<h1>-- P4wn3d --</h1>')");
```

- Embed the “.swf” file to the excel file to run on *file open*. Steps to embed the flash file:
 - Open a new Excel sheet. From the ‘View’ menu select ‘Toolbars’ then ‘Control Toolbox’. The toolbox should appear on your screen.
 - Click the ‘spanner and hammer’ icon on the ‘Control Toolbox’. A dropdown ListView window will popup.
 - From the window that appears, scroll down and select the item called “Shockwave Flash Object”. Click and drag the object to resize it on the excel file.
 - Click on the ‘Properties’ button on the ‘Control Toolbox’ toolbar.
 - In the window that appears select Custom (at the top of the list), and then click the button with 3 dots on it.
 - In the dialog box that appears type the full path of the flash file
 - Tick the checkbox to Embed Movie.
 - Deselect the Loop checkbox.
 - Click the OK button and then close the Properties dialog box.
 - Save the Excel file and reopen, the flash will play on load and run the action scripts.

IV. SOLUTION (PROVIDED BY MICROSOFT)

Just like IE - Microsoft Office enforces ActiveX control kill bits for SFI controls. In fact the same OS kill bit infrastructure used by IE is also used in Office. To learn more about kill bits please see <http://support.microsoft.com/kb/240797/EN-US/>.

Office XP, 2003 honor kill bits - that is if an attacker tries to instantiate a malicious control that has already had a kill bit issued then they will be unsuccessful. Customer may also create their own kill bits by reviewing the KB article listed above.

We are considering making changes in upcoming version and SP's to better flag warn or control embedded controls.

V. DISCLOSURE TIMELINES

03 / 05 / 2006 -	Vendor reported
05 / 05 / 2006 -	Vendor requested for more info
09 / 05 / 2006 -	More details with a working exploit provided to vendor
11 / 05 / 2006 -	Vendor confirmed the issue and requested for more time to investigate
18 / 05 / 2006 -	Vendor came up with the temporary workaround
23 / 05 / 2006 -	Vendor requested to get the advisory past through MSRC before public release
27 / 05 / 2006 -	Vendor suggested minor changes in the advisory
27 / 05 / 2006 -	Vendor requested to hold the advisory till 20th June
20 / 06 / 2006 -	Vendor approved the release of advisory
20 / 06 / 2006 -	Public disclosure

VI. CREDITS

Debasis Mohanty (aka Tr0y)

www.hackingspirits.com

d3basis.m0hanty@gmail.com

Sample-xls-embed-flash.xls is included as a demo PoC.