

Vulnerability Advisory

Name	Unchecked buffer in mstask.dll
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/MS04-022.msp
Date Released	July 14, 2004
Affected Software	Microsoft Windows 2000 Service Pack 4 Microsoft Windows XP, Microsoft Windows XP Service Pack 1
Researcher	Brett Moore brett.moore@security-assessment.com

Description

When thinking about buffer overflow vulnerabilities, a file can sometimes be as harmful as a packet. Even though past security issues have taught us that it is unwise to use an unvalidated text string containing a file name or directory, that is what happened here.

By creating a .job file with a large "to be executed" field the stack can be overwritten allowing for remote command execution, when the file is parsed by mstask.dll.

Details

It appears that both explorer.exe and iexplore.exe will parse a .job file when showing folder listings. Upon the parsing of the .job file, the large "to be executed" field is passed to wcsncpy without doing any bounds checking.

Using explorer the viewing of a folder containing the .job is enough to cause the buffer overflow to occur. The file can be hosted locally or on a remote network share. A remote attack would require the end user to visit the folder/share containing the exploit file.

Using Internet Explorer the viewing of a folder containing the .job file through the use of an [iframe] object will cause the buffer overflow to occur.

Viewing an HTML email that is based around the [iframe] attack avenue, will also cause the buffer overflow. This will occur without any user intervention if the preview pane is enabled, or with user intervention by viewing the email. It is possible that there are other avenues of attack to exploit this vulnerability.

Exploitation

Remote exploitation through Internet Explorer can be obtained through the use of an iframe object pointing at an anonymous share.

Automatic exploitation of browser based bugs, does not rely on an attacker sending a link, requiring the target user to click on it. Links, references and other objects can easily be opened through script code. And I am told that this can also be achieved without script code.

Solution

Install the vendor supplied patch.

<http://www.microsoft.com/technet/security/bulletin/MS04-022.msp>

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com

Email info@security-assessment.com

Phone +649 302 5093