

Vulnerability Advisory

Name	Explorer WebView – Arbitrary Code Execution
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS05-049.msp
Date Released	October 11, 2005
Affected Software	Microsoft Windows 2000
Researcher	Brett Moore brett.moore@security-assessment.com

Description

When webview is enabled on windows 2000 and the \winnt\tasks folder is opened, the web pane shows some information from the currently selected .job file.

In particular the creator field is included in the panes HTML. There is no filtering here, and this allows the addition on arbitrary HTML into the local zone.

This is very similar to

<http://www.microsoft.com/technet/security/Bulletin/MS05-024.msp>

Exploitation

Remote exploitation through Internet Explorer can be obtained through hosting a malicious .job file and constructing a share that points to the folder containing it. Local HTML can be used to run any executable through the use of the codebase method, or other scripting functionality.

Solution

Install the vendor supplied patch.

<http://www.microsoft.com/technet/security/Bulletin/MS05-049.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