



## Vulnerability Advisory

<b>Name</b>	MS Interactive Training .cbo Overflow
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/bulletin/MS07-005.msp">http://www.microsoft.com/technet/security/bulletin/MS07-005.msp</a>
<b>Date Released</b>	February 14, 2007
<b>Affected Software</b>	Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows Server 2003
<b>Researcher</b>	Brett Moore <a href="mailto:brett.moore@security-assessment.com">brett.moore@security-assessment.com</a>

### Overview

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 a string from a file/packet without first checking its length, this is what happened here.

MS Interactive Training will open a file with a .cbo extension and read in the Syllabus details.

Through the creation of a corrupt file, with a long Syllabus string it is possible to gain control of EIP and execute arbitrary code.

```
[Microsoft Interactive Training]
Topic=Using the Start Menu
Lesson=Getting Started with Windows XP Professional
User=DEFAULT
Syllabus=<long string>
Database=C:\Documents and Settings\All Users\Application Data\SBSI\ORUN\
SerialID=00000000
```

### Exploitation

Remote exploitation through Internet Explorer can be obtained through hosting a malicious .cbo file which will be downloaded and opened automatically.

### Solutions

Install the vendor supplied patch.

<http://www.microsoft.com/technet/security/bulletin/MS07-005.msp>

### About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs.

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

Web [www.security-assessment.com](http://www.security-assessment.com)  
Email [info@security-assessment.com](mailto:info@security-assessment.com)  
Phone +649 302 5093