



Vulnerability Advisory

Name	MS Interactive Training .cbo Overflow
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS05-031.msp
Date Released	June 14, 2005
Affected Software	Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows Server 2003 Microsoft Windows 98
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 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 user details.

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

```
[Microsoft Interactive Training]
User=<long string>
SerialID=00000000
```

Exploitation

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

Solution

Install the vendor supplied patch.

<http://www.microsoft.com/technet/security/Bulletin/MS05-031.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

