

## Vulnerability Advisory

<b>Name</b>	Buffer Overflow In HyperTerminal
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/bulletin/MS04-043.msp">http://www.microsoft.com/technet/security/bulletin/MS04-043.msp</a>
<b>Date Released</b>	December 15, 2004
<b>Affected Software</b>	Microsoft Windows NT Server 4.0 SP 6a Microsoft Windows NT Server 4.0 Terminal Server Edition SP6 Microsoft Windows 2000 SP4 Microsoft Windows XP SP2 Microsoft Windows XP 64-Bit Edition SP1 Microsoft Windows XP 64-Bit Edition Version 2003 Microsoft Windows Server 2003 Microsoft Windows Server 2003 64-Bit Edition
<b>Researcher</b>	Brett Moore <a href="mailto:brett.moore@security-assessment.com">brett.moore@security-assessment.com</a>

### 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.

HyperTerminal will save sessions as files with the extension of .ht which will contain the connection info for the current session. It is then possible to have the connection restarted by loading or executing the saved session file. Through the creation of a corrupt .ht file, it is possible to gain control of EIP and execute arbitrary code.

### Exploitation

It appears that a section of the heap, that is overwritten with the corrupt file, contains a lookup table that is later used through a CALL [ECX+374] instruction. This allows for exploitation even on systems like XP SP2, as the stack/heap protection does not come into play.

Basic exploitation can be achieved through sending the target user the corrupt file. Once the file is opened, and HyperTerminal is closed any arbitrary code will be executed.

Remote exploitation through Internet Explorer can be obtained through the use of an iframe or other similar object to open a file from a public UNC share or through a 'coupled' browser exploit that saves the file to a known location before opening it. If HyperTerminal is the current default telnet handler, Internet Explorer will automatically open the corrupt file, leading to exploitation.

There did appear to be some URL manipulation that caused the \ character to be altered, preventing the use of the UNC share, but this filtering could be prevented by the use of another valid URL character.

### Solution

Install the vendor supplied patch.

<http://www.microsoft.com/technet/security/bulletin/MS04-043.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 our 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](http://www.security-assessment.com)  
Email [info@security-assessment.com](mailto:info@security-assessment.com)  
Phone +649 302 5093