security-assessment.com

Vulnerability Advisory

Name	Utilman Loads Winhlp32 As System
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS04-011.mspx
Date Released	April 14, 2004
Affected Software	Microsoft Windows 2000
Researcher	Brett Moore brett.moore@security-assessment.com

Description

The utility manager has had many privilege escalation vulnerabilities in the past related to 'shatter attacks'. While investigating for more attack avenues it was discovered that utility manager will load a winhlp32 process without dropping privileges. This winhlp32 process could then be attacked and SYSTEM privileges obtained.

Although it drops privileges when loading help files through the 'help' button, if the F1 key or the ? button were used to received context sensitive help, winhlp32.exe is loaded with system privileges.

Winhlp32.exe loads as a hidden window, which can then be exploited by sending GDI messages to it.

We discovered various 'undocumented' messages used by winhlp32 including one message that will pass an address of a structure containing function pointers. By sending an address of our buffer, execution flow could be redirected into our buffer.

Cesar Cerrudo, discovered this independently and exploited the winhlp32 process through a different set of messages method.

Both of these methods allow for a local user to execute code with SYSTEM level rights.

Solution

Install the vendor supplied patch.
http://www.microsoft.com/technet/security/Bulletin/MS04-011.mspx

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