

Security-Assessment.com – Security Alert

Name	HTML Help API - Privilege Escalation
Date Released	October 24, 2003
Affected Software	Microsoft Windows NT Microsoft Windows 2000 Microsoft Windows 2003 Microsoft Windows XP
Researcher	Brett Moore brett.moore@security-assessment.com

Background

Microsoft Windows allows applications to use a standard method of displaying and handling help files. One of these methods is using the HTML help API.

HTML Help API Overview

The HTML Help application programming interface (API) enables a Windows program to create a help window that displays a help topic. The Windows program has complete control over the type, style, and position of the help window.

The fundamental feature of the HTML Help API is the help window. Through the API commands, you can create a help window that hosts a Microsoft Internet Explorer DLL (Shdocvw.dll) and displays an HTML file that you specify.

The HTML help API consists of one function that an application uses to pass commands.

```
HWND HtmlHelp(  
    HWND hwndCaller,  
    LPCSTR pszFile,  
    UINT uCommand,  
    DWORD dwData) ;
```

When an application loads a help file using this function it passes the name of the file through the pszFile parameter. It appears that this function does not drop any privileges before invoking the help viewer.

If a SYSTEM level application uses this function to display a help file, the HTML help viewer will be running with SYSTEM rights.

Part of the help window consists of an instance of Internet Explorer which allows a user to browse the local drive.

By selecting jump to URL from the window system menu, a user can enter a path name (c:\), right-mouse-click on a file and then select open with cmd.exe to be given a SYSTEM level command shell window.

Example Vulnerable Programs

From our testing, any application running at a higher security level that invokes htmlhelp without dropping privileges is vulnerable. We tested various Personal Firewall and Antivirus applications and found some to be vulnerable to this attack. We found no 'default' windows applications vulnerable to this attack, but think that it is something that application developers need to be aware of.

Security-Assessment

.com

Solutions

The HTML help view (hh.exe) should be called externally passing the helpfile name as a parameter.

Security rights could be dropped through the use of `system()` or `CreateProcess()` functions. `CreateProcessAsUser()` or `ImpersonateLoggedOnUser()` could be used to control the rights that `htmlhelp` executes with.

If an interactive window requires SYSTEM rights, its functionality should be limited to those functions requiring the higher level of privilege.

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