

[NT] HtmlHelp CHM File Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0060.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/14/04

To: list@securiteam.com

Date: 14 Jul 2004 18:24:32 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

HtmlHelp CHM File Heap Overflow

SUMMARY

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 an invalidated value from a file/packet as a text length parameter that is what happened here.

The HtmlHelp application (hh.exe) will read a value from a .CHM file and use this as the 'length' parameter in a REPZ MOVSD operation. By setting this to a large value, it is possible to overwrite sections of the heap with attacker-supplied values.

This results in a typical win32 heap overflow landing either on the common `mov [ecx],eax / mov [eax+4],ecx` pair, or on a `call [eax+4]`. In either case the registers are under the control of the attacker leading to code execution.

DETAILS

Vulnerable Systems:

- * Microsoft Windows 98, 98SE, ME
- * Microsoft Windows NT 4.0
- * Microsoft Windows 2000 Service Pack 4

Securiteam: [NT] HtmlHelp CHM File Heap Overflow

- * Microsoft Windows XP, Microsoft Windows XP Service Pack 1
- * Microsoft Windows Server 2003

When the corrupt file is opened an exception error will first occur at:
0x78010044 REPZ MOVSD

The error has occurred because the destination address has reached the end of its allocated space. After clicking OK on the popup error box, execution will continue until it eventually reaches.

```
0x77fcc663 mov [ecx],eax
0x77fcc665 mov [eax+4],ecx
```

At this time the EAX and ECX values have been filled with the data used to overwrite the heap, allowing an attacker to write an arbitrary value to a known place.

The corrupt file must be constructed in such a way to jump through some hoops first. It must pass some checks reliant on a value in the file that sets ESI.

- * This value must be valid memory
- * [ESI+1c] must be non NULL
- * [ESI+24] must be NULL

This value is simple to achieve resulting in a reliable heap exploit using any of the multiple methods now known to exploit heap overflows.

Exploitation:

Remote exploitation through Internet Explorer can be obtained through the use of the window.showhelp() function. Either using a public UNC shares or through a 'coupled' browser exploit that saves the file to a known location before opening it. There may of course also be other ways of having a corrupt .CHM file loaded without requiring a user to download and run it, although a compiled help file may be easily accepted by a user anyway.

Automatic exploitation of browser based bugs, does not rely on an attacker sending a link, requiring the target user to click on it. Links, references and other objects can easily be opened through script code. And Brett was told that this could also be achieved without script code.

Patch Availability:

For patch details see our previous article:

<<http://www.securiteam.com/windowsntfocus/5TP0A15DGQ.html>> Vulnerability in HTML Help Could Allow Code Execution (MS04-023).

ADDITIONAL INFORMATION

The information has been provided by
<mailto:brett.moore@security-assessment.com> Brett Moore.

=====

Securiteam: [NT] HtmlHelp CHM File Heap Overflow

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.