

# HtmlHelp – .CHM File Heap Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-07/0034.html>

---

**From:** Brett Moore (*brett.moore\_at\_SECURITY-ASSESSMENT.COM*)

**Date:** 07/14/04

Date: Wed, 14 Jul 2004 17:37:05 +1200  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

=====  
= HtmlHelp – .CHM File Heap Overflow  
=  
= MS Bulletin posted:  
=<http://www.microsoft.com/technet/security/bulletin/MS04-023.msp>  
=  
= Affected Software:  
= Microsoft Windows 98, 98SE, ME  
= Microsoft Windows NT 4.0  
= Microsoft Windows 2000 Service Pack 4  
= Microsoft Windows XP, Microsoft Windows XP Service Pack 1  
= Microsoft Windows Server 2003  
=  
= Public disclosure on July 14, 2004  
=====

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 unvalidated 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.

== Description ==

When the corrupt file is opened an exception error will first occur at

0x78010044 REPZ MOVSD

## NT-Bugtraq: HtmlHelp – .CHM File Heap Overflow

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 share 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 I am told that this can also be achieved without script code.

== Solutions ==

- Install the vendor supplied patch.

== Credit ==

Discovered and advised to Microsoft January 12, 2004 by Brett Moore of Security-Assessment.com

%-) Well Ruxcon rocked, so gotta say thanks to all that were there. They %-) known who they are. Now for vegas....

== About Security-Assessment.com ==

NT-Bugtraq: HtmlHelp – .CHM File Heap Overflow

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.

#####  
CONFIDENTIALITY NOTICE:

This message and any attachment(s) are confidential and proprietary. They may also be privileged or otherwise protected from disclosure. If you are not the intended recipient, advise the sender and delete this message and any attachment from your system. If you are not the intended recipient, you are not authorised to use or copy this message or attachment or disclose the contents to any other person. Views expressed are not necessarily endorsed by Security-Assessment.com Limited. Please note that this communication does not designate an information system for the purposes of the New Zealand Electronic Transactions Act 2003.

#####

-----  
NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.

-----