

Bad string handling in hha.dll (HTML Help Workshop)?

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-05/0001.html>

From: Chad Myers (*cmyers_at_AUSTIN.RR.COM*)

Date: 05/16/05

Date: Mon, 16 May 2005 15:33:09 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Everyone:

Sorry I can't provide more details about this issue. I'm hoping one of the technical folks that know how to identify and exploit a possible vulnerability like this can help track down the specifics. It appears there is some bad string handling in (what appears to be) hha.dll that is part of the HTML Help Compiler (HHC.exe) and/or HTML Help Workshop (version 4.74.8702.0 on my system). I'm not sure, but this might be a buffer overrun and could be exploitable.

We use a tool to generate all the files necessary for the HHC to spit out a resultant CHM file. The tool had a bug in it that spit out a file name that was greater than MAX_PATH. The tool could not save the file. It failed silently, but it added the path to the T.O.C. file that HHC uses.

When HHC went to compile, it tried to read the too-big file name and it crashed with an access violation (0xc0000005 - Access Violation).

Here are some details:

VERSIONS

=====

OS: WinXP SP2

HHW: 4.74.8702.0

HHA: 4.74.8702.0

HHCTRL: 5.02.3790.1280

ITIRCL: 5.02.3790.1159

ITSS: 5.02.3790.1221

I was able to get Dr Watson to dump some interesting information, perhaps this will help:

-----> State Dump for Thread Id 0x10d4 <-----

eax=00000000 ebx=00000000 ecx=ffffffff edx=45381228 esi=682e296e

NT-Bugtraq: Bad string handling in hha.dll (HTML Help Workshop)?

edi=682e296e eip=4530f3fb esp=0012ec90 ebp=0012ecb0 iopl=0
nv up ei pl zr na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 fl=00000246

*** ERROR: Symbol file could not be found. Defaulted to export symbols for
C:\WINDOWS\system32\HHA.dll -

function: HHA!Ordinal23
4530f3e4 53 push ebx
4530f3e5 56 push esi
4530f3e6 8b74240c mov esi,[esp+0xc]
4530f3ea 57 push edi
4530f3eb 85f6 test esi,esi
4530f3ed 7505 jnz HHA!Ordinal23+0x10 (4530f3f4)
4530f3ef bee4363645 mov esi,0x453636e4
4530f3f4 8bfe mov edi,esi
4530f3f6 83c9ff or ecx,0xffffffff
4530f3f9 33c0 xor eax,eax
FAULT ->4530f3fb f2ae repne scasb

es:682e296e=??
4530f3fd f7d1 not ecx
4530f3ff 51 push ecx
4530f400 e86b290300 call HHA!Ordinal358+0x4d3 (45341d70)
4530f405 59 pop ecx
4530f406 8bd0 mov edx,eax
4530f408 8bfe mov edi,esi
4530f40a 83c9ff or ecx,0xffffffff
4530f40d 33c0 xor eax,eax
4530f40f f2ae repne scasb
4530f411 f7d1 not ecx

-----> Stack Back Trace <-----

WARNING: Stack unwind information not available. Following frames may be wrong.

ChildEBP RetAddr Args to Child
0012ecb0 45315376 682e296e 00000000 0012eef8 HHA!Ordinal23+0x17
0012ed1c 4531beaa 682e296e 0012ed3c 00000000 HHA!Ordinal315+0x1d
0012ef4c 4531e702 0012f3b4 00ca2c20 0012ef7c HHA!HHA_CompileHHP+0x36fe
006c6d74 00000013 00000000 7fffffff 00000000 HHA!HHA_CompileHHP+0x5f56

-----> Raw Stack Dump <-----

000000000012ec90 00 00 00 00 ec ec 12 00 - 00 00 00 00 aa 4c 31 45
000000000012eca0 6e 29 2e 68 00 00 00 00 - f8 ee 12 00 00 00 00 00
000000000012ecb0 1c ed 12 00 76 53 31 45 - 6e 29 2e 68 00 00 00 00
000000000012ecc0 f8 ee 12 00 14 f6 12 00 - a0 2d ca 00 00 00 00 00
000000000012ecd0 a0 2d ca 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000000012ece0 00 00 00 00 00 00 00 00 - 00 00 d5 77 e0 2c ca 00
000000000012ecf0 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000000012ed00 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 31 45
000000000012ed10 80 ef 12 00 9c 21 36 45 - ff ff ff ff 4c ef 12 00
000000000012ed20 aa be 31 45 6e 29 2e 68 - 3c ed 12 00 00 00 00 00

NT-Bugtraq: Bad string handling in hha.dll (HTML Help Workshop)?

```
000000000012ed30 20 2c ca 00 27 2c ca 00 - 18 f1 12 00 46 43 68 6f
000000000012ed40 69 63 65 2e 54 6f 6f 6c - 6b 69 74 73 2e 43 6c 61
000000000012ed50 72 69 66 79 7e 46 43 68 - 6f 69 63 65 2e 54 6f 6f
000000000012ed60 6c 6b 69 74 73 2e 43 6c - 61 72 69 66 79 2e 49 6e
000000000012ed70 74 65 72 66 61 63 65 73 - 2e 49 6e 74 65 72 66 61
000000000012ed80 63 65 73 54 6f 6f 6c 6b - 69 74 7e 43 72 65 61 74
000000000012ed90 65 51 75 65 75 65 28 53 - 74 72 69 6e 67 2c 42 6f
000000000012eda0 6f 6c 65 61 6e 2c 42 6f - 6f 6c 65 61 6e 2c 42 6f
000000000012edb0 6f 6c 65 61 6e 2c 42 6f - 6f 6c 65 61 6e 2c 42 6f
000000000012edc0 6f 6c 65 61 6e 2c 42 6f - 6f 6c 65 61 6e 2c 42 6f
```

I hope this helps someone.

Sincerely,
Chad Myers

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--