Vulnerability Advisory

Name	ASP.DLL Include File Buffer Overflow
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS06-034.mspx
Date Released	July 19, 2006
Affected Software	IIS 5.0 IIS 5.1 IIS 6.0
Researcher	Brett Moore brett.moore@security-assessment.com

Overview

A buffer overflow exists in ASP.DLL that can be exploited by creating a .asp file containing a parameter for the include SSI command.

```
<!-- #include file="<long buffer>" -->OVERFLOWDATA
```

The include function in ASP.DLL, checks if the parameter is longer than 260 bytes. If it is then an error is caused, but before causing the error a miscalculated copy is done.

```
mov     edi, [ebp+var_228]   ; load length of parameter
cmp     edi, 104h            ; check if larger than 260 bytes
jbe     short loc_
mov     esi, [ebp+var_22C]   ; load address of parameter
lea     eax, [edi+esi-104h]  ; load eax with the address of the last
                             ; 260 bytes of the parameter
                             ; (length of string+source of string)- 104h
lea     edx, [ebp+var_211]   ; load edx with address on stack
sub     edx, eax             ;
mov     cl, [eax]            ;  \
mov     [edx+eax], cl        ;   do the copy
inc     eax                  ;   and overflow the stack
test    cl, cl               ;  /
jnz     short loc_7096D1F3   ;
```

Funnily enough, the solution was to remove this copy as the resulting data was never actually used.

Exploitation

Exploitation requires the ability to upload or somehow create a file with a .asp extension in a folder that will allow .asp processing.

Since ASP.DLL usually runs under the IWAM_ account, there is no privilege escalation through this vulnerability. It is however possible to bypass any security restrictions enforced by ASP. It also allows for the execution of APIS that have no ASP equivalent.

Solution

Install the vendor supplied upgrade;
http://www.microsoft.com/technet/security/Bulletin/MS06-034.mspx

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.