Security-Assessment.com – Vulnerability Advisory

Name	Listbox And Combobox Control Buffer Overflow
Microsoft Advisory	http ://www.microsoft.com/technet/security/bulletin/ms03-045.asp
Date Released	October 15, 2003
Affected Software	Microsoft Windows NT 4.0 Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows 2003
Researcher	Brett Moore brett.moore@security-assessment.com

Description
As past history has shown us, Windows has many buffer overflows resulting from the mishandling of long file names or path names. This one is no different.

Sending either a LB_DIR message to a listbox or a CB_DIR message to a combobox, specifying a large pathname as the parameter will result in the receiving application stopping with an access violation error, resulting in the following log message.

```
Event Type:     Error
Event Source:   Service Control Manager
Event Category:None
Event ID:       7031
Description:
The [application] service terminated unexpectedly.
```

At the time of the error, attacker supplied data is been used as the application execution point. By controlling this an attacker can execute their own commands.
On Windows 2000, the utility manager runs under the localsystem account and contains a listbox control that will accept messages from unprivileged users, allowing for the escalation of privileges to localsystem level.

Solutions

Install the vendor supplied patch.
http://www.microsoft.com/technet/security/bulletin/ms03-045.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

The LB_DIR and CB_DIR messages are defined as;

LB_DIR
An application sends an LB_DIR message to add a list of filenames to a list box
wParam = (WPARAM) (UINT) uAttrs; // file attributes
lParam = (LPARAM) (LPCTSTR) lpszFileSpec; // filename address
lpszFileSpec
Value of lParam. Pointer to the null-terminated string that specifies the filenames
CB_DIR
An application sends a CB_DIR message to add a list of filenames to a combo box.
wParam = (WPARAM) (UINT) uAttrs; // file attributes
lParam = (LPARAM) (LPCTSTR) lpszFileSpec; // address of filename
lpszFileSpec
Value of lParam. Pointer to the null-terminated string that specifies the filenames

The following details are based on the exploitation of the utility manager on windows 2000.

After sending a message with a large pathname utilman will cause an exception within a call to wcscpy.

The exception occurs at this code location;
```
77F81E98   mov        dx,word ptr [ecx]
77F81E9B   mov        word ptr [esi],dx   <-- Exception
```

At this point ESI has been incremented to much and is now pointing to an invalid memory location. The registers look like this;
EAX = 007AF6DC EBX = 0000018D
ECX = 007E0924 EDX = 0000FFFF
ESI = 007B0000 EDI = 007E0000
EIP = 77F81E9B ESP = 007AF6AC
EBP = 007AFD6C EFL = 00000286

The area where the pathname has been copied to starts at 0x007AF6F7,which is higher than ESP, but lower than EBP. The memory starting at EBP now contains the data passed in the pathname, and any future reference to EBP will reference this data.
```
007AFD6C  58 58 58 58 58  XXXXX
007AFD71  58 58 58 58 58  XXXXX
```

Because an exception has occurred, and our pathname has overwritten the exception handlers on the stack, an unhandled exception will occur when execution flow reaches;
```
77F8EB6B   mov        ecx,dword ptr [ebp+18h]         <-- EBP points to buffer
77F8EB6E   call       ecx                  <-- We control ECX
```

At this point EBX points directly into the buffer and by correctly forming the pathname, execution flow can be directed back into our buffer.

Standard stack based overflow techniques apply and exploits can be written for either Unicode or non-Unicode depending on which API is used to send the original message.

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