security-assessment.com

Vulnerability Advisory

Name	SetWindowLong Shatter Attacks
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx
Date Released	October 14, 2004
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 explained in my presentation at Blackhat earlier this year, attacks against the windows GUI do not stop with sending messages. In that presentation I talked about the exploitative usage of the SetProp() API method. The SetWindowLong()/SetWindowLongPtr() API's can also be used to exploit certain applications for arbitrary advantage.

Background

The SetWindowLong() function is documented in MSDN as;

The SetWindowLong function changes an attribute of the specified window. The function also sets a 32-bit (long) value at the specified offset into the extra window memory of a window.

```
LONG SetWindowLong(
  HWND hWnd,       // handle of window
  int nIndex,      // offset of value to set
  LONG dwNewLong   // new value
);
```

Parameters

hWnd

Handle to the window and, indirectly, the class to which the window belongs.

nIndex

Specifies the zero-based offset to the value to be set. Valid values are in the range zero through the number of bytes of extra window memory, minus 4; for example, if you specified 12 or more bytes of extra memory, a value of 8 would be an index to the third 32-bit integer.

To set any other value, specify one of the following values:

Value	Action
GWL_EXSTYLE	Sets a new extended window style.
GWL_STYLE	Sets a new window style.
GWL_WNDPROC	Sets a new address for the window procedure.
GWL_HINSTANCE	Sets a new application instance handle.
GWL_ID	Sets a new identifier of the window.
GWL_USERDATA	Sets the 32-bit value associated with the window. Each window has a corresponding 32-bit value intended for use by the application that created the window.

The following values are also available when the hWnd parameter identifies a dialog box:

Value	Action
DWL_DLGPROC	Sets the new address of the dialog box procedure.
DWL_MSGRESULT	Sets the return value of a message processed in the dialog box procedure.
DWL_USER	Sets new extra information that is private to the application, such as handles or pointers.

dwNewLong

Specifies the replacement value.

Remarks
The SetWindowLong function fails if the window specified by the hWnd parameter does not belong to the same process as the calling thread.

The functions compliment is the GetWindowLong() function, which is used to retrieve a value.

Even though the remarks section is documented as written above, it is not a true statement.

As with the SendMessage() function (as used by standard shatter attacks) any user can call the etWindowLong() function to alter the data stored in the window memory.

Exploitation

We founds multiple third party and core windows services that used the memory space pointed to by the GWL_USERDATA, to store specific data. In some cases this data could be manipulated to gain execution control.

Since each application stores different information in this memory and therefore the exploitation differs, we can not explain them all. We will however give a quick example of how execution control could be obtained.

We discovered that [Service X], that did not normally have a window, could be enticed into generating an error that would display a window. The service stored a pointer to a lookup table in the window memory pointed to by GWL_USERDATA. This lookup table held the address of functions, and was later used to retrieve an address and pass it to a CALL instruction.

By using the process mapped heap, as explained in my Blackhat presentation, it was possible to place our shellcode into a known location. We could also construct a new lookup table, pointing to our shellcode, in a known location.

Then by using SetWIndowLongPtr() API we replaced the pointer to the lookup table with the address of our new lookup table. The service would use our lookup table and execution would therefore reach the shellcode.

Solution

Install the vendor supplied patch.
http://www.microsoft.com/technet/security/bulletin/ms04-032.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.

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

Copyright Security-Assessment.com Ltd 2004