[NT] ListBox and ComboBox Control Buffer Overflow (Technical Details)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2003−10/0082.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 10/19/03

```
To: list@securiteam.com
Date: 19 Oct 2003 17:04:41 +0200
```

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: http://www.securiteam.com
− − promotion

The SecuriTeam alerts list − Free, Accurate, Independent.

Get your security news from a reliable source.
http://www.securiteam.com/mailinglist.html

− − − − − − − − −

ListBox and ComboBox Control Buffer Overflow (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 filename to add to the list

CB_DIR
An application sends a CB_DIR message to add a list of filenames to the list box of 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 filename to add to the list

Exploitation:
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.

The following details are based on the exploitation of that ListBox.

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

* From MSDN *
strcpy, wcscpy Copy a string.
char *strcpy(char *strDestination, const char *strSource);
wchar_t *wcscpy(wchar_t *strDestination, const wchar_t *strSource);

Parameters
strDestination − Destination string
strSource − Null−terminated source string

Remarks
The strcpy function copies strSource, including the terminating null character, to the location specified by strDestination. No overflow checking is performed when strings are copied or appended.
* End MSDN *

The exception occurs at this code location;
77F81E98 mov dx,word ptr [ecx]
77F81E9B mov word ptr [esi],dx <−− Exception
77F81E9E inc esi
77F81E9F inc esi

77F81EA0 inc ecx
77F81EA1 inc ecx
77F81EA2 test dx,dx
77F81EA5 jne 77F81E98

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
007AFD76 58 58 58 58 58 XXXXX
007AFD7B 58 58 58 58 58 XXXXX
007AFD80 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.

Solutions:
− Install the vendor supplied patch available at
<http://www.securiteam.com/windowsntfocus/6O00H1P8KU.html>
http://www.securiteam.com/windowsntfocus/6O00H1P8KU.html.
− Interactive processes should not run under a higher level account.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:brett.moore@security−assessment.com> Brett Moore.

==========

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:

list−unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list−subscribe@securiteam.com

==========
==========

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.