

# CredUICmdLinePromptForCredentialsW stack overflow issue

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-10/0145.html>

---

**From:** Skywing (*skywing\_NO\_SPAM\_\_at\_valhallalegends.com*)

**Date:** 10/20/05

Date: Thu, 20 Oct 2005 12:34:53 -0400

There is a bug (race condition it seems) that causes CredUICmdLinePromptForCredentialsW to sometimes enter an infinite recursive loop when called, eventually causing the calling problem to stack overflow and die.

This is visible on Windows XP SP2 Professional English (with all patches applied).

You can reproduce this problem using RunAs.exe by creating a shell shortcut (in explorer) to "%systemroot%\system32\runas.exe /smartcard cmd.exe" and then executing the shortcut from explorer. This appears to be a race condition; attaching a debugger to explorer with child debugging enabled prevents the problem from occurring, and running the shortcut from IE in explorer mode also (usually) prevents the problem from occurring.

(You do not actually have to have a smartcard reader installed for CredUICmdLinePromptForCredentialsW to crash like this.)

The symptoms after following the repro steps are that runas just instantly "goes away" after starting. If you use gflags to set a debugger in ImageFileExecutionOptions (I used WinDbg), you can trap the stack overflow and get a stack trace.

On the machines I'm seeing this on, I'm seeing something like this:

```
(9e0.a8c): Stack overflow - code c00000fd (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00007450 ebx=00020886 ecx=0003ce60 edx=7c90eb94 esi=00000000
edi=77d488a6
eip=76c05818 esp=00042e5c ebp=0004307c iopl=0         nv up ei pl nz na po
nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000
efl=00010206
credui!CreduiCredentialControl::MessageHandler+0x10:
76c05818 53 push ebx
```

```
0:000> kvnf 0x1000
# Memory ChildEBP RetAddr Args to Child
00 0004307c 76c06145 00000127 00030001 00000000
credui!CreduiCredentialControl::MessageHandler+0x10 (FPO: [Non-Fpo])
01 20 0004309c 77d48734 00020886 00000127 00030001
credui!CreduiCredentialControl::MessageHandlerCallback+0x2b (FPO: [Non-Fpo])
02 2c 000430c8 77d48816 76c0611a 00020886 00000127
USER32!InternalCallWinProc+0x28
03 68 00043130 77d4b89b 00094b38 76c0611a 00020886
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])
04 3c 0004316c 77d4b903 00564ee0 00564ba8 00030001
USER32!SendMessageWorker+0x4a5 (FPO: [Non-Fpo])
05 20 0004318c 76c079f9 00020886 00000127 00030001
USER32!SendMessageW+0x7f (FPO: [Non-Fpo])
06 18 000431a4 76c07ed1 00000127 00030001 00000000
credui!CreduiPasswordDialog::CmdLineMessageHandler+0x17 (FPO: [Non-Fpo])
07 20 000431c4 77d48734 00020888 00000127 00030001
credui!CreduiPasswordDialog::CmdLineMessageHandlerCallback+0x2a (FPO:
[Non-Fpo])
08 2c 000431f0 77d48816 76c07ea7 00020888 00000127
USER32!InternalCallWinProc+0x28
09 68 00043258 77d58480 00094b38 76c07ea7 00020888
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])
0a 54 000432ac 77d4b3f9 00020886 00000001 00000000
USER32!RealDefWindowProcWorker+0x12eb (FPO: [Non-Fpo])
0b 1c 000432c8 77d4b393 00020886 00000127 00030001
USER32!RealDefWindowProcW+0x47 (FPO: [Non-Fpo])
0c 48 00043310 76c05cbd 00020886 00000127 00030001
USER32!DefWindowProcW+0x72 (FPO: [Non-Fpo])
0d 244 00043554 76c06145 00000127 00030001 00000000
credui!CreduiCredentialControl::MessageHandler+0x4b5 (FPO: [Non-Fpo])
0e 20 00043574 77d48734 00020886 00000127 00030001
credui!CreduiCredentialControl::MessageHandlerCallback+0x2b (FPO: [Non-Fpo])
```

```
.
.
.
[snip – similar stack frames repeated for many frames]
```

```
.
.
.
9ac 18 0007c9f4 76c07ed1 00000127 00030001 00000000
credui!CreduiPasswordDialog::CmdLineMessageHandler+0x17 (FPO: [Non-Fpo])
9ad 20 0007ca14 77d48734 00020888 00000127 00030001
credui!CreduiPasswordDialog::CmdLineMessageHandlerCallback+0x2a (FPO:
[Non-Fpo])
9ae 2c 0007ca40 77d48816 76c07ea7 00020888 00000127
USER32!InternalCallWinProc+0x28
9af 68 0007caa8 77d58480 00094b38 76c07ea7 00020888
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])
```

9b0 54 0007cafc 77d4b3f9 00020886 00000001 00000000  
USER32!RealDefWindowProcWorker+0x12eb (FPO: [Non-Fpo])  
9b1 1c 0007cb18 77d4b393 00020886 00000127 00030001  
USER32!RealDefWindowProcW+0x47 (FPO: [Non-Fpo])  
9b2 48 0007cb60 76c05cbd 00020886 00000127 00030001  
USER32!DefWindowProcW+0x72 (FPO: [Non-Fpo])  
9b3 244 0007cda4 76c06145 00000127 00030001 00000000  
credui!CreduiCredentialControl::MessageHandler+0x4b5 (FPO: [Non-Fpo])  
9b4 20 0007cdc4 77d48734 00020886 00000127 00030001  
credui!CreduiCredentialControl::MessageHandlerCallback+0x2b (FPO: [Non-Fpo])  
9b5 2c 0007cdf0 77d48816 76c0611a 00020886 00000127  
USER32!InternalCallWinProc+0x28  
9b6 68 0007ce58 77d58480 00094b38 76c0611a 00020886  
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])  
9b7 54 0007ceac 77d4b3f9 0002087c 00000001 00000000  
USER32!RealDefWindowProcWorker+0x12eb (FPO: [Non-Fpo])  
9b8 1c 0007cec8 77d4b393 0002087c 00000127 00000003  
USER32!RealDefWindowProcW+0x47 (FPO: [Non-Fpo])  
9b9 48 0007cf10 773f9606 0002087c 00000127 00000003  
USER32!DefWindowProcW+0x72 (FPO: [Non-Fpo])  
9ba 98 0007cfa8 77d48734 0002087c 00000127 00000003  
comctl32!Button\_WndProc+0xab0 (FPO: [Non-Fpo])  
9bb 2c 0007cfd4 77d48816 773f8b56 0002087c 00000127  
USER32!InternalCallWinProc+0x28  
9bc 68 0007d03c 77d4b89b 00094b38 773f8b56 0002087c  
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])  
9bd 3c 0007d078 77d4b903 005652f8 00563c38 00000003  
USER32!SendMessageWorker+0x4a5 (FPO: [Non-Fpo])  
9be 20 0007d098 773f9233 0002087c 00000127 00000003  
USER32!SendMessageW+0x7f (FPO: [Non-Fpo])  
9bf 98 0007d130 77d48734 0002087c 00000001 00000000  
comctl32!Button\_WndProc+0x6dd (FPO: [Non-Fpo])  
9c0 2c 0007d15c 77d48816 773f8b56 0002087c 00000001  
USER32!InternalCallWinProc+0x28  
9c1 68 0007d1c4 77d4b4c0 00094b38 773f8b56 0002087c  
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])  
9c2 54 0007d218 77d4fd29 005652f8 00000001 00000000  
USER32!DispatchClientMessage+0xa3 (FPO: [Non-Fpo])  
9c3 30 0007d248 7c90eae3 0007d258 00000070 00000070  
USER32!\_\_fnINLPCREATESTRUCT+0x8b (FPO: [Non-Fpo])  
9c4 7c 0007d2c4 77d5013e 77d50104 00000004 0007d7ec  
ntdll!KiUserCallbackDispatcher+0x13 (FPO: [0,0,0])  
9c5 4a4 0007d768 77d501f7 00000004 0007d7ec 0007d800  
USER32!NtUserCreateWindowEx+0xc  
9c6 ac 0007d814 77d4ff83 00000004 76c01420 0007d800  
USER32!\_CreateWindowEx+0x1ed (FPO: [Non-Fpo])  
9c7 3c 0007d850 76c0c85b 00000004 76c01420 76c01430  
USER32!CreateWindowExW+0x33 (FPO: [Non-Fpo])  
9c8 64 0007d8b4 76c03365 00000004 76c01420 76c01430  
credui!SHFusionCreateWindowEx+0x50 (FPO: [Non-Fpo])  
9c9 74 0007d928 76c04ae2 00000000 0003ce60 00000004

credui!CreduiCredentialControl::CreateControls+0x292 (FPO: [Non-Fpo])  
9ca 18 0007d940 76c05882 77d488a6 00000000 00020886  
credui!CreduiCredentialControl::InitWindow+0x35 (FPO: [Non-Fpo])  
9cb 234 0007db74 76c06145 00001001 00000004 00000001  
credui!CreduiCredentialControl::MessageHandler+0x7a (FPO: [Non-Fpo])  
9cc 20 0007db94 77d48734 00020886 00001001 00000004  
credui!CreduiCredentialControl::MessageHandlerCallback+0x2b (FPO: [Non-Fpo])  
9cd 2c 0007dbc0 77d48816 76c0611a 00020886 00001001  
USER32!InternalCallWinProc+0x28  
9ce 68 0007dc28 77d4b89b 00094b38 76c0611a 00020886  
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])  
9cf 3c 0007dc64 77d4b903 00564ee0 00564ba8 00000004  
USER32!SendMessageWorker+0x4a5 (FPO: [Non-Fpo])  
9d0 20 0007dc84 76c06eb4 00020886 00001001 00000004  
USER32!SendMessageW+0x7f (FPO: [Non-Fpo])  
9d1 5c 0007dce0 76c07eea 00000000 0007dd60 76c07ea7  
credui!CreduiPasswordDialog::InitWindow+0x3b9 (FPO: [Non-Fpo])  
9d2 18 0007dcf8 77d48734 00020888 00000001 00000000  
credui!CreduiPasswordDialog::CmdLineMessageHandlerCallback+0x43 (FPO:  
[Non-Fpo])  
9d3 2c 0007dd24 77d48816 76c07ea7 00020888 00000001  
USER32!InternalCallWinProc+0x28  
9d4 68 0007dd8c 77d4b4c0 00094b38 76c07ea7 00020888  
USER32!UserCallWinProcCheckWow+0x150 (FPO: [Non-Fpo])  
9d5 54 0007dde0 77d4fd29 00564e30 00000001 00000000  
USER32!DispatchClientMessage+0xa3 (FPO: [Non-Fpo])  
9d6 30 0007de10 7c90eae3 0007de20 00000060 00000060  
USER32!\_\_fnINLPCREATESTRUCT+0x8b (FPO: [Non-Fpo])  
9d7 6c 0007de7c 77d5013e 77d50104 00000000 0007e3a4  
ntdll!KiUserCallbackDispatcher+0x13 (FPO: [0,0,0])  
9d8 4a4 0007e320 77d501f7 00000000 0007e3a4 00000000  
USER32!NtUserCreateWindowEx+0xc  
9d9 ac 0007e3cc 77d4ff83 00000000 76c01538 00000000  
USER32!\_CreateWindowEx+0x1ed (FPO: [Non-Fpo])  
9da 3c 0007e408 76c0c7e6 00000000 76c01538 00000000  
USER32!CreateWindowExW+0x33 (FPO: [Non-Fpo])  
9db 64 0007e46c 76c08205 76c01538 00000000 80000000  
credui!SHFusionCreateWindow+0x4e (FPO: [Non-Fpo])  
9dc 88 0007e4f4 76c08a5e 77c47e94 77c47fcc 0000000e  
credui!CreduiPasswordDialog::CmdLineDialog+0xac (FPO: [Non-Fpo])  
9dd 34 0007e528 76c09976 0002088a 00000001 00080000  
credui!CreduiPasswordDialog::CreduiPasswordDialog+0x79b (FPO: [Non-Fpo])  
9de 674 0007eb9c 76c09c7e 00000001 00000000 0007ec4c  
credui!CredUIPromptForCredentialsWorker+0x1fd (FPO: [Non-Fpo])  
9df 34 0007ebd0 01001727 0007ec4c 00000000 00000000  
credui!CredUICmdLinePromptForCredentialsW+0x29 (FPO: [Non-Fpo])  
9e0 44 0007ec14 01002179 00000001 0007f454 00000100  
runas!GetCredentials+0x168 (FPO: [Non-Fpo])  
9e1 1308 0007ff1c 010025d3 00000003 00000000 00092366  
runas!WinMain+0x579 (FPO: [4,1204,3])  
9e2 a4 0007ffc0 7c816d4f 00080000 0090fa9c 7ffd6000

microsoft.public.platformsdk.security: CredUICmdLinePromptForCredentialsW stack overflow issue  
runas!WinMainCRTStartup+0x174 (FPO: [Non-Fpo])