Jabber per Windows Crash Dump Analysis con lo strumento WinDbg

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Esegui analisi dettagli arresto anomalo per Cisco Jabber per Windows Configurazione simboli WinDbg Analisi dettagli arresto anomalo in WinDbg

Introduzione

Questo documento descrive la procedura usata per analizzare il file **.dmp** creato quando si blocca il client Cisco Jabber for Windows.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Jabber per Windows.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Jabber per Windows versione 9.x e Cisco Unified Personal Communicator (CUPC) versione 8.6.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esegui analisi dettagli arresto anomalo per Cisco Jabber per Windows

Usare lo strumento WinDbg per eseguire l'analisi dei dettagli dell'arresto anomalo del sistema. Scaricare lo strumento dal <u>sito Web WinDbg.</u>

Configurazione simboli WinDbg

- 1. Per modificare il percorso del simbolo, selezionate File > Percorso file di simboli > Percorso simbolo.
- 2.
- 3. Incolla il testo nella finestra:

SRV*c:\websymbols*http://msdl.microsoft.com/download/symbols

- 4.
- 5. Fare clic su OK.

Analisi dettagli arresto anomalo in WinDbg

1. Avviare WinDbg.

WinDbg:6.2.9200.16384 X86						-		83
File Edit View Debug Window Help								
12 X 电局 面 图 图 10 P						B (101	AA
r								
Ln 0,	Col 0	Sys 0: <none></none>	Proc 000:0	Thrd 000:0	ASM	OVR	CAPS	NUM
		-					-	

2.

3. Dal menu File, fare clic su Apri dettagli arresto anomalo.

WinDbg:6.2.9200.16384 X86					0		×
File Edit View Debug Window	Help						
Open Source File Close Current Window	Ctrl+O Ctrl+F4	11100	9 9 0 0			101 101	A,
Open Executable Attach to a Process	Ctrl+E F6						
Open Crash Dump	Ctrl+D						
Connect to Remote Session Connect to Remote Stub	Ctrl+R						
Kernel Debug	Ctrl+K						
Symbol File Path	Ctrl+S						
Source File Path	Ctrl+P						
Image File Path	Ctrl +I						
Open Workspace Save Workspace Save Workspace As Clear Workspace Delete Workspaces Open Workspace in File Save Workspace to File	Ctrl+W						
Map Network Drive							
Disconnect Network Drive							
Recent Files	•						
Exit	Alt+F4	Sys 0: <none></none>	Proc 000:0	Thrd 000:0	ASM OV	R CAPS	NU

4. Scegliere il file **.dmp** (memory.dmp, user.dmp, ecc.) e fare clic su **Apri** o trascinare il file **.dmp** in WinDbg. In questo esempio viene utilizzato il file **fulldump**.



5.

6. Nella finestra dei comandi in basso, immettere **!analyze - v**, quindi premere **Invio**.



7.

8. Il progresso dell'analisi è visibile nella parte inferiore sinistra dello schermo. In questa immagine, lo stato è "OCCUPATO".

- 0 23 Dump C:\Users\asishtla\Desktop\chris jones\fulldump.dmp - WinDbg:6:2.9200.16384 X86 Edit View Debug Window Help File Cô. Command - Dump C:\Users\asishtla\Desktop\chris jones\fulldump.dmp - WinDbg:6.2.9200.1638... Loading unloaded module list ٠ eax=03c64370 ebx=00000001 ecx=00000002 edx=00000000 esi=0013fdb0 edi=0013fd94 eip=776f7094 esp=0013fc94 ebp=0013fcb0 iopl=0 cs=001b ss=0023 ds=0023 es=0023 fs=003b e nv up ei pl zr na pe nc es=0023 fs=003b gs=0000 ef1=00000246 ntdll!KiFastSystemCallRet: 776f7094 c3 ret 0:000> !analyze -v Exception Analysis WARNING: Unable to verify timestamp for CiscoJabber.exe Module load completed but symbols could not be loaded for CiscoJabb *** ERROR: *** WARNING: Unable to verify timestamp for JabberUtils.dll Module load completed but symbols could not be loaded for JabberUti *** ERROR: *** WARNING: Unable to verify timestamp for msvcr90.dll *** WARNING: Unable to verify timestamp for VoicemailService.dll *** ERROR: Module load completed but symbols could not be loaded for Voicemail *** WARNING: Unable to verify timestamp for servicesframework.dll *** ERROR: Module load completed but symbols could not be loaded for servicesf: *BUSY* Ln 0, Col 0 Sys 0:C:\User Proc 000:11b4 Thrd 000:197c ASM OVR CAPS NUM

Questo comando esegue un'analisi con una visualizzazione completamente dettagliata dei dati ed è utile per ottenere ulteriori informazioni.

9.

10. Per uscire, immettere q nella finestra di comando e premere Invio.

Di seguito è riportato un esempio di output dell'analizzatore di dump:

```
> !analyze -v
<snip>
STACK_TEXT:
WARNING: Frame IP not in any known module. Following frames may be wrong.
02f4e80c 01457967 7ffdac00 00000104 02f4e86c 0x0
02f4e848 0145637d 0000001 02f4e86c 02f4ed58 wxvault+0x7967
02f4ea88 7c8138b7 7ffdac00 0000000 02f4eac8 wxvault+0x637d
02f4ed1c 009a436f 00b413b4 02f4ed58 0000000
kernel32!FindFirstFileA+0x3a
02f4edb8 00000000 00000000 00000000 CUPCK9+0x5a436f
STACK_COMMAND: ~8s; .ecxr ; kb
SYMBOL_STACK_INDEX: 1
SYMBOL_NAME: wxvault+7967
```

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: wxvault

IMAGE_NAME: wxvault.dll

DEBUG_FLR_IMAGE_TIMESTAMP: 450162c1

FAILURE_BUCKET_ID: NULL_INSTRUCTION_PTR_c0000005_wxvault.dll!Unknown

BUCKET_ID: APPLICATION_FAULT_NULL_INSTRUCTION_PTR_NULL_POINTER_READ_DETOURED_NULL_IP_ wxvault+7967

Esaminare MODULE_NAME e IMAGE_NAME. Le informazioni fornite, ad esempio wxvault.dll o CiscoJabber.exe, indicano l'applicazione che ha causato l'arresto anomalo. In questo caso, l'arresto anomalo si è verificato a causa di problemi con l'applicazione Cisco Jabber.exe e non con il computer dell'utente. Una ricerca effettuata da Google mostra che wxvault.dll è correlato a DELL Embassy Trust Suite.

Inviare il Report di problema di Cisco Jabber al Technical Assistance Center di Cisco per determinare se il dump di arresto anomalo è correlato a un difetto noto con una possibile soluzione.