Análise de despejo de travamento do Jabber para Windows com a ferramenta WinDbg

Contents

Introduction Prerequisites Requirements Componentes Utilizados Executar análise de despejo de falhas para o Cisco Jabber para Windows Configuração dos símbolos WinDbg Análise de despejo de memória no WinDbg

Introduction

Este documento descreve o procedimento usado para analisar o arquivo **.dmp** criado quando o cliente Cisco Jabber para Windows trava.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Cisco Jabber para Windows.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Jabber para Windows versão 9.x e no Cisco Unified Personal Communicator (CUPC) versão 8.6.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Executar análise de despejo de falhas para o Cisco Jabber para Windows

Use a ferramenta WinDbg para executar a análise de despejo de memória. Baixe a ferramenta do

Configuração dos símbolos WinDbg

- 1. Para alterar o caminho do símbolo, navegue para **Arquivo > Caminho do arquivo de** símbolos > Caminho do símbolo.
- 2.
- 3. Colar este texto na janela:

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

- 4.
- 5. Click OK.

Análise de despejo de memória no WinDbg

1. Iniciar WinDbg.



2.

3. No menu Arquivo, clique em Abrir despejo de travamento.

WinDbg:6.2.9200.16384 X86							*
ile Edit View Debug Window	Help		-				
Open Source File Close Current Window	Ctrl+O Ctrl+F4	m 0 0.	9 9 0 0				¦ 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	OVR CAPS	NU

4. Escolha o arquivo **.dmp** (memory.dmp, user.dmp, etc.) e clique em **Abrir** ou arraste e solte o arquivo **.dmp** no WinDbg. Este exemplo usa o arquivo **full dump**.



5.

6. Na janela de comando na parte inferior, digite **!analyze - v** e pressione **Enter**.



7.

8. Você pode ver o progresso da análise na parte inferior esquerda da tela. Nesta imagem, o status é "OCUPADO".

- 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 *** ERROR: Module load completed but symbols could not be loaded for JabberUti *** 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

Esse comando executa uma análise com uma exibição de dados totalmente detalhada e é útil para obter mais informações.

9.

10. Para sair, digite q na janela de comando e pressione Enter.

Aqui está um exemplo de saída do analisador de despejo:

```
> !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 00000000 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

Examine o **MODULE_NAME** e o **IMAGE_NAME**. As informações fornecidas, como **wxvault.dll** ou **CiscoJabber.exe**, indicam qual aplicativo causou o travamento. Nesse caso, o travamento ocorreu devido a problemas com o aplicativo Cisco Jabber.exe e não com a máquina do usuário. Uma pesquisa do Google mostra que **wxvault.dll** está relacionado ao pacote de confiança da Embaixada da DELL.

Envie o Relatório de Problemas do Cisco Jabber para o Centro de Assistência Técnica da Cisco para determinar se o dump de travamento está relacionado a um defeito conhecido que tenha uma possível solução alternativa.