

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe un problema encontrado cuando el proceso del windump se utiliza con el marcador saliente del Cisco Unified Contact Center Enterprise (UCCE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco UCCE
- Session Initiation Protocol (SIP) de la versión 8.x de Cisco UCCE o marcador del protocolo skinny client control (SCCP)

Componentes Utilizados

La información en este documento se basa en el marcador saliente del Cisco Unified Contact Center Enterprise (UCCE).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Cuando se ven los registros salientes del proceso del marcador, usted observa que el proceso del windump causa un crash cada 15 segundos:

```
-----  
13:00:12:615 dialer-baDialer Trace: WinDump process has crashed, restarting...  
13:00:12:617 dialer-baDialer Trace: CreateProcess succeeded with szCmdline = windump -I 1  
-tt -C 20 -s 0 -W 20 -w DialerCapture udp port 58800  
dwProcessId= 262600 hProcess = 256784
```

```
13:00:28:843 dialer-baDialer Trace: WinDump process has crashed, restarting...
13:00:28:844 dialer-baDialer Trace: CreateProcess succeeded with szCmdline = windump -I 1
-tt -C 20 -s 0 -W 20 -w DialerCapture udp port 58800
dwProcessId= 262412 hProcess = 256792
13:00:45:069 dialer-baDialer Trace: WinDump process has crashed, restarting...
-----
```

Cuando el windump causa un crash en varias ocasiones, lleva a una situación de la fuga de memoria que los resultados en una caída saliente del servicio del marcador.

Solución

Hay un par de escenarios que pudieron llevar a este problema:

- La clave de registro saliente del marcador de las **opciones de la captura** no se fija correctamente. Navegue a `\ HKEY_LOCAL_MACHINE \ SOFTWARE \ Cisco Systems, Inc. \ > \ marcador del caso ICM \ del <Customer` y asegurese que la clave de registro de las **opciones de la captura** está fijada - i1 - al tt - C20 - s0 - W 20 - w DialerCapture.

En algunas situaciones, la clave de registro se fija - i1 - al tt - C20 - s0 - W 20 - w **DialerCapture**, que da lugar a una caída. Esto se ve a menudo cuando el marcador saliente se actualiza de una versión anterior. Para más detalles, refiera al Id. de bug Cisco [CSCuh16754](#) (el proceso del windump causa un crash en el marcador).

- El software de Wireshark pudo afectar a los archivos de biblioteca dinámicamente enlazados capturados (DLL). Si Wireshark está instalado en el servidor para resolver problemas, y posterior desinstalado, el retiro del WinPcap por la desinstalación puede llevar a este problema. El proceso de la desinstalación de Wireshark quita los DLL capturados **wpcap.dll** y **packet.dll**, que el windump requiere.

Para confirmar que los archivos necesarios están presentes y que el windump trabaja correctamente, complete estos pasos:

1. Asegurese el **wpcap.dll** y el **Packet.dll**files están presente en estas ubicaciones:
C:\Windows\SysWOW64\C:\Windows\System32Si los archivos DLL no se encuentran, entre en contacto el Centro de Asistencia Técnica de Cisco (TAC) para obtener las versiones correctas de los archivos DLL.
2. Para confirmar que el proceso del windump está instalado y captura correctamente los datos correctamente, examine la salida de estos comandos: `c:\>windump -v`

```
windump version 3.9.5, based on tcpdump version 3.9.5
WinPcap version 4.1.2 (packet.dll version 4.1.0.2001), based on libpcap version 1.0 branch
1_0_rel10b (20091008)
```

```
C:\>windump
```

```
windump: listening on \Device\NPF_{5A01EA28-AF57-4456-A653-DD785A20853F}
13:06:20.596189 IP PG2B.43005 > PG2A.domain.net.49220:
.3075400616:3075400617(1) ack 1040704317 win
13:06:20.596222 IP PG2A.domain.net.49220 > PG2B.43005:
.ack 1 win 255 <nop,nop,sack 1 {0:1}>
13:06:20.606477 IP PG2A.domain.net.49208 > PG2B.45005:
.1242670277:1242670278(1) ack 357439054 win 2
13:06:20.607219 IP PG2B.45005 > PG2A.domain.net.49208:
.0:1(1) ack 1 win 251
```