

# Solucionar problemas cuando Jabber no puede procesar el contenido de Chatbot

## Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

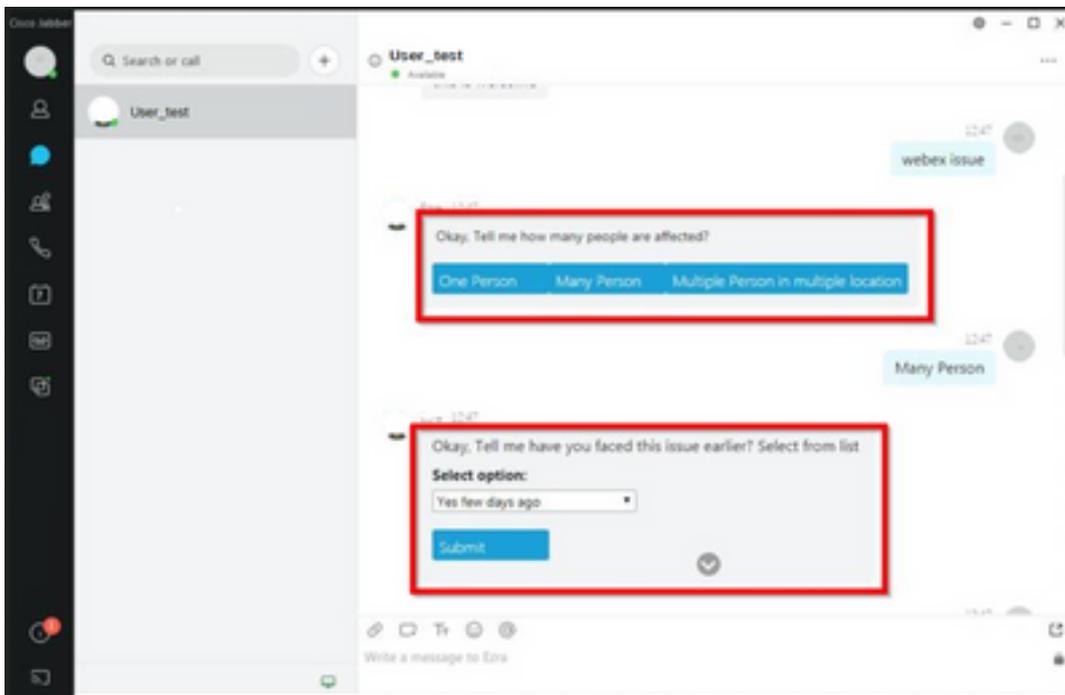
## Introducción

Este documento describe cómo resolver problemas de Cisco Jabber con el procesamiento del contenido del chatbot después de la modificación del código Jabber.

## Antecedentes

Los clientes Jabber pueden incluir Cisco Jabber Bot, desarrollado con un kit de desarrollo de software (SDK) que proporciona un marco y un kit de herramientas para implementar bots de conversación interactivos en la plataforma de mensajes de mensajería instantánea y presencia (IM&P) de Cisco o Cisco Webex Messenger Server. Hay ciertas etiquetas HTML (Lenguaje de marcado de hipertexto) que se pueden configurar para obtener un bot básico de Jabber.

Si la versión de Jabber es 12.9.4 o anterior, el chatbot se ve como se muestra en la imagen, y Jabber tiene la capacidad de mostrar todos los botones y opciones descritos en el código de fuente.



## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- Cisco Jabber
- SDK para bots de Cisco Jabber

### Componentes Utilizados

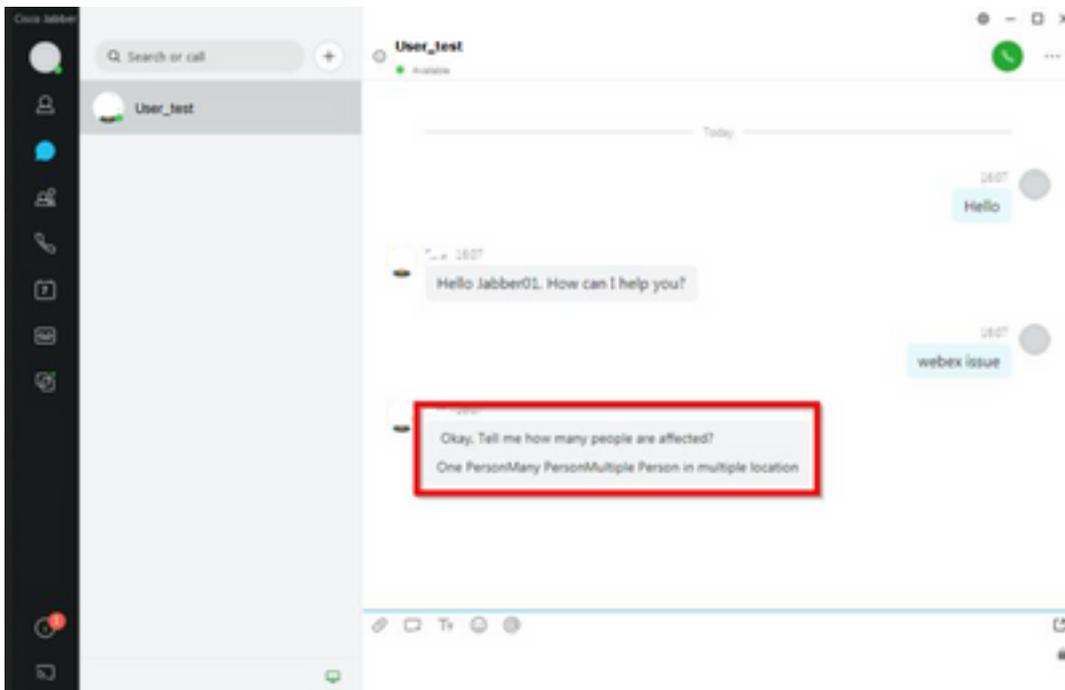
La información que contiene este documento se basa en estas versiones de software y hardware.

- Jabber versión 12.9.X.
- Jabber versión 14.X.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Problema

Si la versión del cliente Jabber es 12.9.5, 14.0 o posterior, debido a las vulnerabilidades publicadas el pasado marzo de 2022 ([CVE-2020-3155](#)), Jabber no puede procesar el contenido de los chatbots ya que muestran el contenido HTML en la interfaz cliente.



Esa función hace que Jabber sea vulnerable a los ataques de las técnicas de hombre en el medio (MITM) para interceptar el tráfico entre el cliente afectado y un terminal, y luego usar un certificado falsificado para suplantar el terminal. Una vulnerabilidad podría permitir al atacante ver el contenido de la presentación compartido en ella, modificar cualquier contenido presentado por la víctima o tener acceso a controles de llamada. Esto depende de la configuración del punto final.

Debido a esta vulnerabilidad, los desarrolladores han introducido una regla de seguridad para permitir que varios elementos para Jabber en las etiquetas de código HTML formen el chatbot.

Antes de la vulnerabilidad, no se realizaban comprobaciones de seguridad para el mensaje bot, pero después del último cambio de seguridad de la vulnerabilidad, el mensaje bot ahora se comprueba mediante los nuevos mecanismos de seguridad.

La regla de seguridad consta de las siguientes etiquetas permitidas y atributos de estilo.

Etiquetas que se permiten.

```
{ "span", "font", "a", "br", "strong", "em", "u", "div", "table", "tbody", "tr", "td", "h1", "h2", "h3", "h4", "h5", "h6", "b", "p", "i", "blockquote", "ol", "li", "ul", "pre", "code" }
```

Atributos de estilo permitidos.

```
{ "font", "text-decoration", "color", "font-weight", "font-size", "font-family", "font-style" }
```

Etiquetas no permitidas.

```
{ "label", "button", "select", "form" }
```

## Solución

Si la declaración de bot de Cisco Jabber tiene algunas o todas las etiquetas no permitidas mencionadas anteriormente, la solución consiste en borrar esas etiquetas del código HTML. Sin embargo, si son necesarios para que el bot funcione, se requiere una clave de configuración.

Para evitar cualquier vulnerabilidad al mismo tiempo, es posible utilizar el chatbot clásico creado con los atributos de estilo y las etiquetas permitidas mencionadas.

Desde la corrección de seguridad de Jabber, no se pueden aceptar todos los demás estilos de fuente o atributos fuera de la lista de permitidos. Por lo tanto, debe cambiar los atributos en el chatbot solamente para incluirlos.

Si todavía necesita utilizar el chatbot normalmente, significa que, con las etiquetas no permitidas, hay una clave de configuración de opción de procesamiento HTML que se puede agregar al archivo `jabber-config.xml` (archivo de configuración de Jabber).

- `hardening_xmpp_bot`: establézcalo en "FALSE" como en la línea de ejemplo.

Ejemplo: `<hardening_xmpp_bot>FALSE</hardening_xmpp_bot>`

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshoot

Actualmente no hay información de troubleshooting específica disponible para esta configuración.

## Información Relacionada

- [Asistencia técnica y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).