Solucionar problemas quando o Jabber não puder renderizar o conteúdo do Chatbot

Contents

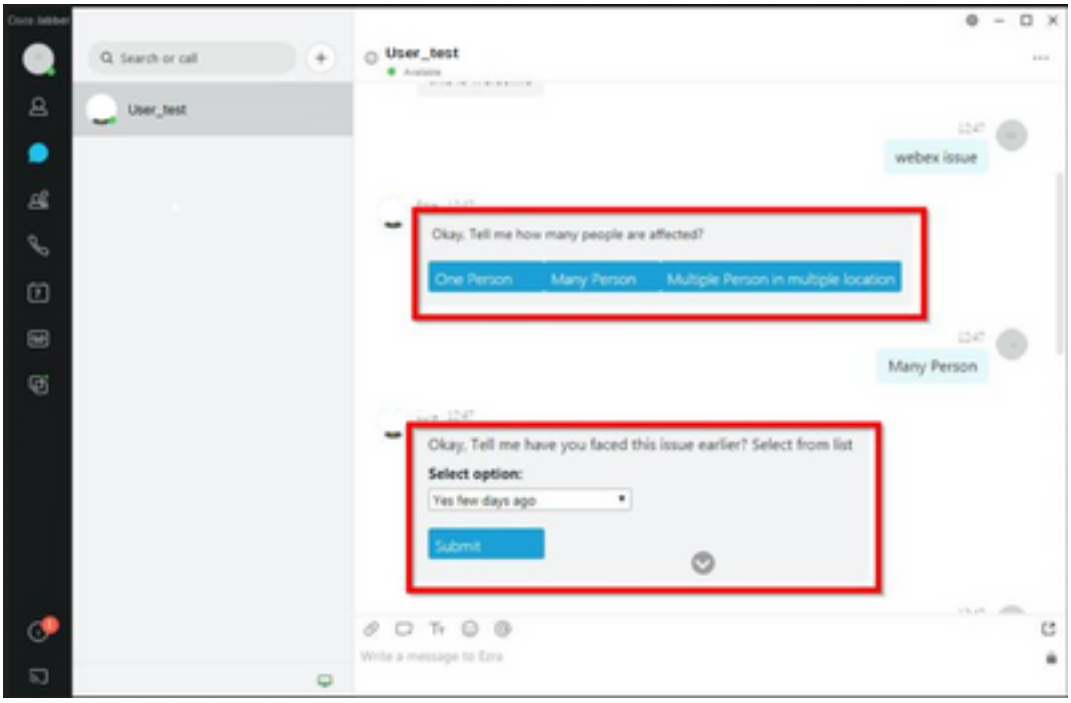
Introduction

Este documento descreve como solucionar problemas do Cisco Jabber com a renderização do conteúdo do chatbot após a modificação do código Jabber.

Informações de Apoio

Os clientes Jabber têm a capacidade de incluir o Cisco Jabber Bot, desenvolvido com um kit de desenvolvimento de software (SDK) que fornece uma estrutura e um kit de ferramentas para implementar bots interativos de conversação na plataforma de mensagens do Cisco Instant Messaging and Presence (IM&P) ou no Cisco Webex Messenger Server. Há certas tags HTML (HyperText Markup Language) que podem ser configuradas para obter um boot Jabber básico.

Se a versão do Jabber for 12.9.4 ou anterior, o chatbot será semelhante ao mostrado na imagem, e o Jabber poderá mostrar todos os botões e opções descritos no código da fonte.



Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos.

- Cisco Jabber
- SDK do Cisco Jabber Bot

Componentes Utilizados

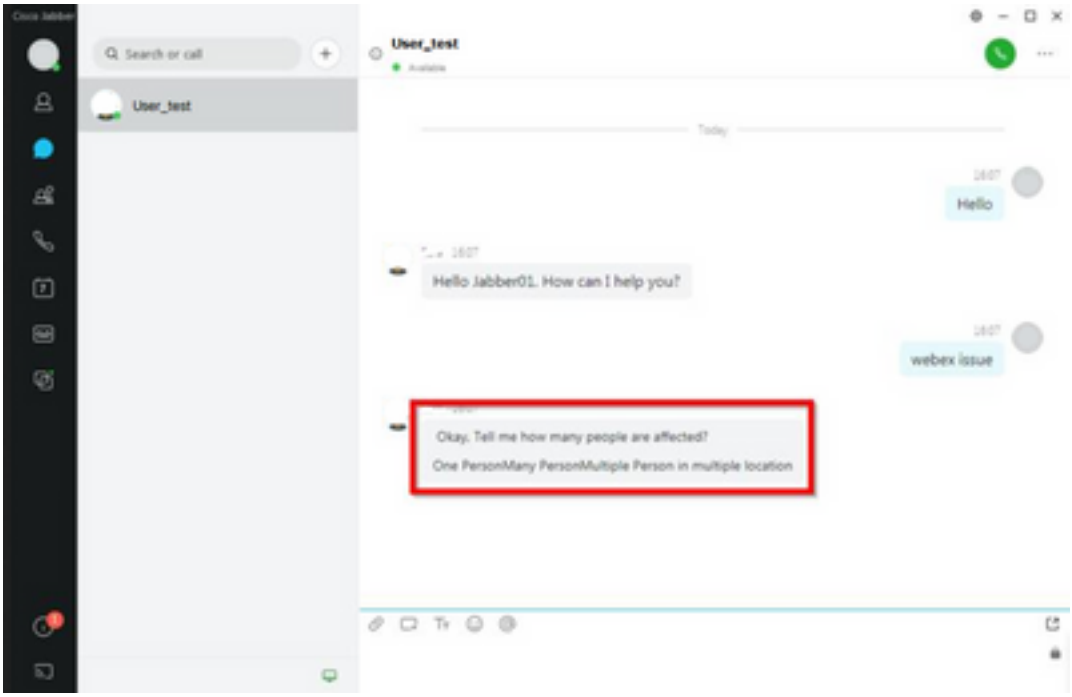
As informações neste documento são baseadas nestas versões de software e hardware.

- Jabber versão 12.9.X.
- Jabber versão 14.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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Se a versão do cliente Jabber for 12.9.5, 14.0 ou posterior, devido às vulnerabilidades publicadas em março de 2022 (CVE-2020-3155), o Jabber agora é incapaz de renderizar o conteúdo dos chatbots à medida que exibem o conteúdo HTML na interface do cliente.



Essa função torna o Jabber vulnerável a ataques de técnicas MITM (man in the middle) para interceptar o tráfego entre o cliente afetado e um endpoint e, em seguida, usar um certificado forjado para representar o endpoint. Uma exploração pode permitir que o invasor visualize o conteúdo de apresentação compartilhado nele, modifique qualquer conteúdo apresentado pela vítima ou tenha acesso aos controles de chamada. Isso depende da configuração do endpoint.

Devido a essa vulnerabilidade, os desenvolvedores introduziram uma regra de segurança para permitir que vários elementos para Jabber nas tags de código HTML formassem o chatbot.

Antes da vulnerabilidade, não havia verificações de segurança para a mensagem de inicialização, mas depois da última alteração de segurança de vulnerabilidade, a mensagem de inicialização é verificada pelos novos mecanismos de segurança.

A regra de segurança consiste nas próximas tags e atributos de estilo permitidos.

Marcas permitidas.

```
{"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"}
```

Marcas não permitidas.

```
{“label”, “button”, “select”, “form”}
```

Solução

Se a declaração de inicialização do Cisco Jabber tiver algumas ou todas as marcas não permitidas acima mencionadas, a solução consistirá em apagar essas marcas do código HTML. No entanto, se eles forem necessários para que o boot funcione, uma chave de configuração será

necessária.

Para evitar qualquer vulnerabilidade ao mesmo tempo, é possível usar o chatbot clássico criado com os atributos de estilo e as tags permitidas mencionadas.

Na correção de segurança do Jabber, todos os outros estilos de fonte ou atributos fora da lista permitida não podem ser aceitos. Portanto, você deve alterar os atributos no chatbot somente para incluí-los.

Se você ainda precisar usar o chatbot normalmente, isso significa que, com as tags não permitidas, há uma chave de configuração da opção de renderização HTML que pode ser adicionada ao arquivo **jabber-config.xml** (arquivo de configuração Jabber).

- hardening_xmpp_bot: defina-o como "FALSE", como na linha de exemplo.

Exemplo: **<hardening_xmpp_bot>***FALSE***</hardening_xmpp_bot>**

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

No momento, não há informações específicas de solução de problemas disponíveis para essa configuração.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.