Risoluzione dei problemi quando Jabber non è in grado di eseguire il rendering del contenuto di Chatbot

Sommario

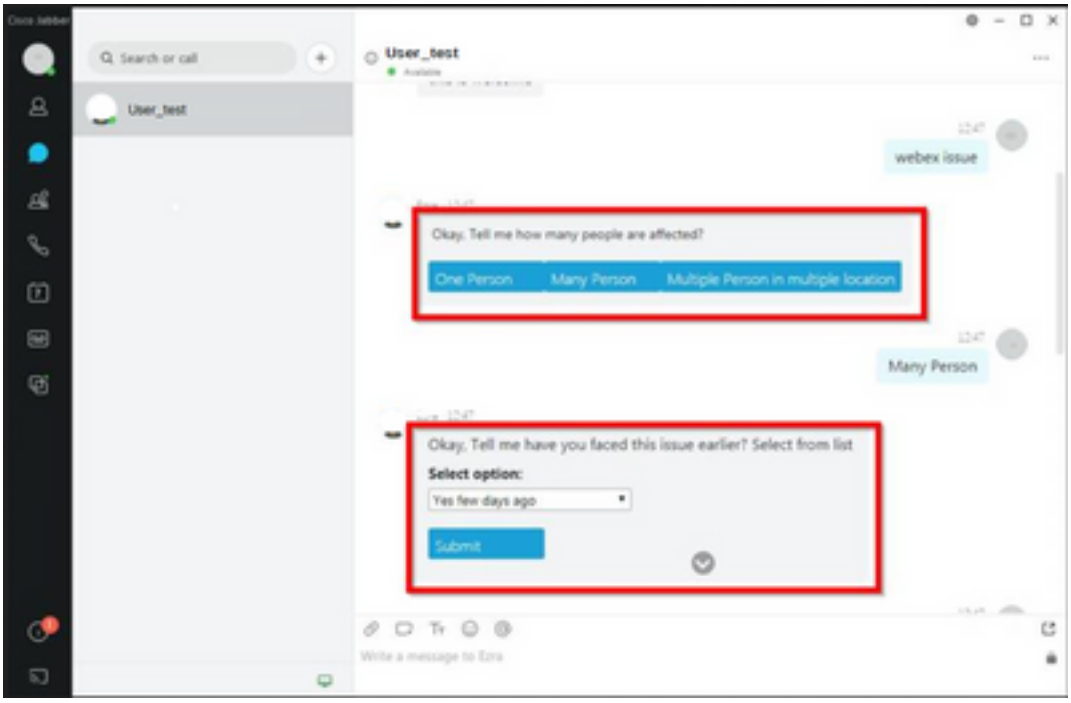
Introduzione

Questo documento descrive come risolvere i problemi di Cisco Jabber con il rendering del contenuto del chatbot dopo la modifica del codice Jabber.

Premesse

I client Jabber hanno la capacità di includere Cisco Jabber Bot, sviluppato con un Software Development Kit (SDK) che fornisce una struttura e un toolkit per implementare i bot conversazionali interattivi sulla piattaforma di messaggi Cisco Instant Messaging and Presence (IM&P) o su Cisco Webex Messenger Server. Alcuni tag HTML (HyperText Markup Language) possono essere configurati per ottenere un avvio Jabber di base.

Se la versione di Jabber è la 12.9.4 o precedente, il chatbot appare come mostrato nell'immagine e Jabber ha la capacità di mostrare tutti i pulsanti e le opzioni descritti nel codice font.



Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- Cisco Jabber
- Cisco Jabber Bot SDK

Componenti usati

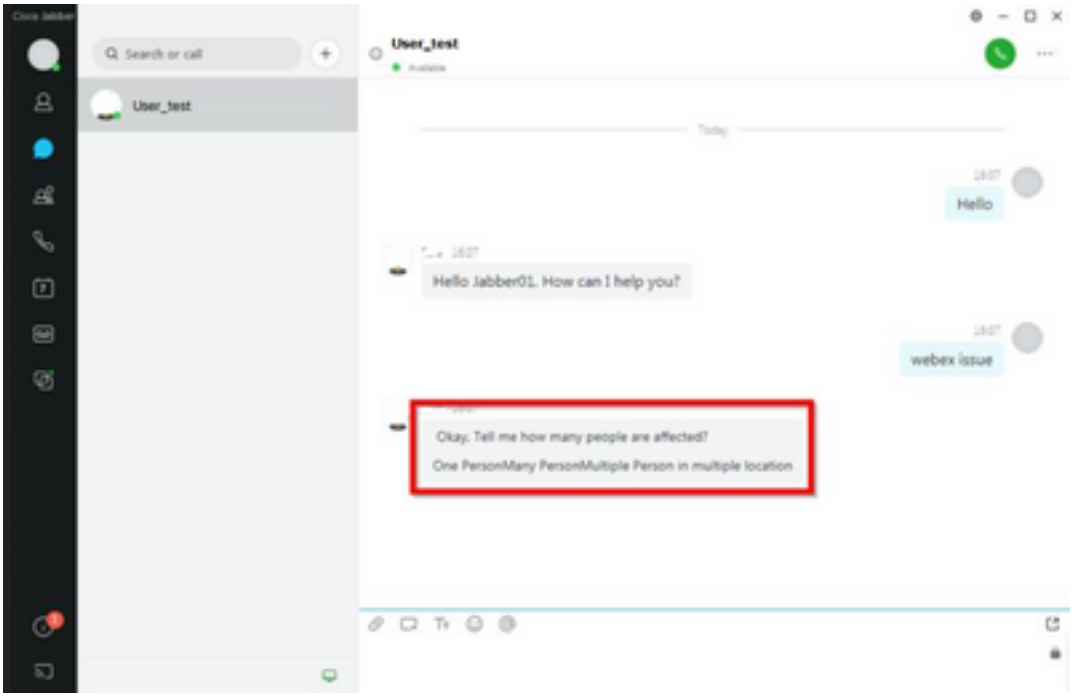
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Jabber versione 12.9.X.
- Jabber versione 14.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.

Problema

Se la versione del client Jabber è la 12.9.5, 14.0 o successiva, a causa delle vulnerabilità pubblicate lo scorso marzo 2022 (CVE-2020-3155), Jabber non è ora in grado di eseguire il rendering del contenuto dei chatbot mentre visualizzano il contenuto HTML nell'interfaccia del client.



Questa funzione rende Jabber vulnerabile agli attacchi delle tecniche MITM (Man in the Middle) per intercettare il traffico tra il client interessato e un endpoint, quindi utilizzare un certificato contraffatto per rappresentare l'endpoint. Un exploit potrebbe consentire all'aggressore di visualizzare il contenuto della presentazione condiviso su di esso, modificare qualsiasi contenuto presentato dalla vittima, o avere accesso ai controlli di chiamata. Ciò dipende dalla configurazione dell'endpoint.

A causa di questa vulnerabilità, gli sviluppatori hanno introdotto una regola di sicurezza per consentire a Jabber di creare il chatbot attraverso i tag di codice HTML.

Prima della vulnerabilità, non c'erano controlli di sicurezza per il messaggio di bot, ma dopo l'ultima modifica di sicurezza della vulnerabilità, il messaggio di bot è ora controllato dai nuovi meccanismi di sicurezza.

La regola di protezione è costituita dai tag e dagli attributi di stile consentiti successivi.

Tag consentiti.

```
{"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"}
```

Attributi di stile consentiti.

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

Tag non consentiti.

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

Soluzione

Se la dichiarazione di avvio di Cisco Jabber include alcuni o tutti i tag non consentiti sopra citati, la soluzione consiste nel cancellare tali tag dal codice HTML. Tuttavia, se sono necessarie per il

funzionamento del robot, è necessaria una chiave di configurazione.

Per evitare qualsiasi vulnerabilità allo stesso tempo, è possibile utilizzare il chatbot classico creato con gli attributi di stile e tag consentiti menzionati.

Dalla correzione rapida per la protezione di Jabber, non è possibile accettare tutti gli altri stili di carattere o attributi non inclusi nell'elenco dei tipi di carattere consentiti. Pertanto, è necessario modificare gli attributi nel chatbot solo per includerli.

Se è ancora necessario utilizzare il chatbot normalmente, significa che con i tag non consentiti è disponibile una chiave di configurazione dell'opzione di rendering HTML che può essere aggiunta al file **jabber-config.xml** (file di configurazione Jabber).

- hardening_xmpp_bot: impostarlo su "FALSE" come nella riga di esempio.

Esempio: **<hardening_xmpp_bot>***FALSE***</hardening_xmpp_bot>**

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

Informazioni correlate

- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).