Troubleshoot when Jabber Unable to Render Chatbot Content

Contents

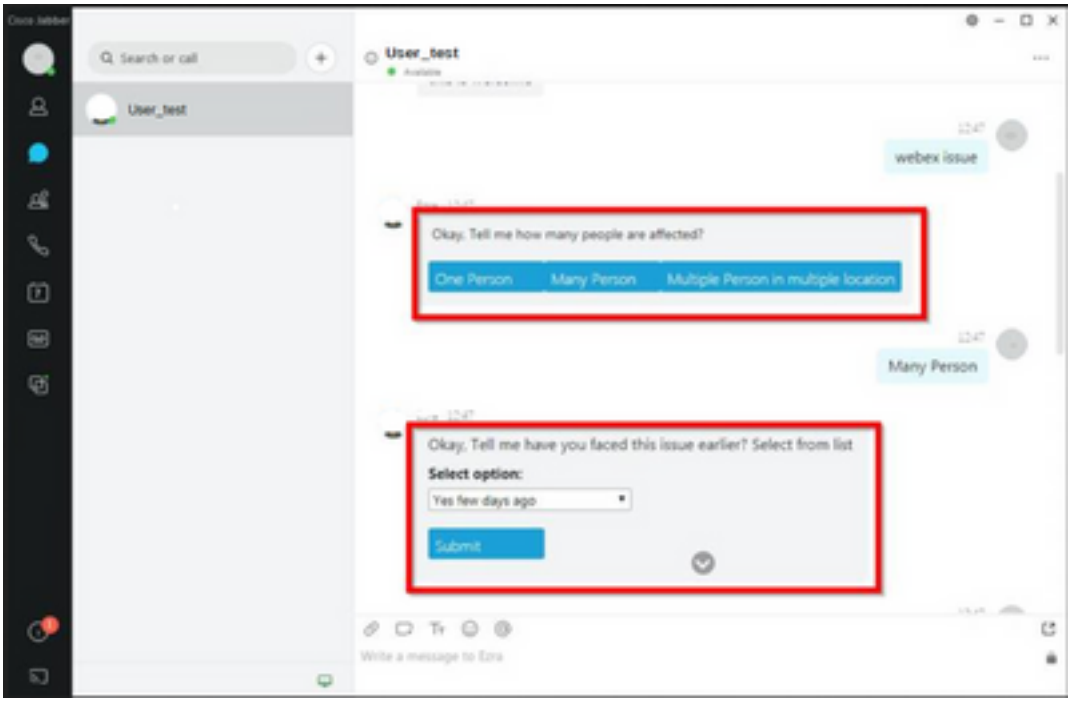
Introduction

This document describes how to troubleshoot Cisco Jabber issues with the render of chatbot content after the Jabber code modification.

Background Information

The Jabber clients have the capability to include the Cisco Jabber Bot, developed with a Software Development Kit (SDK) that provides a framework and toolkit to implement interactive conversational bots on Cisco Instant Messaging and Presence (IM&P) message platform or Cisco Webex Messenger Server. There are certain HyperText Markup Language (HTML) tags that can be configured to get a basic Jabber bot.

If the Jabber version is 12.9.4 or earlier the chatbot looks as shown in the image, and Jabber has the capability to show all buttons and options described in the font code.



Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics.

- Cisco Jabber
- Cisco Jabber Bot SDK

Components Used

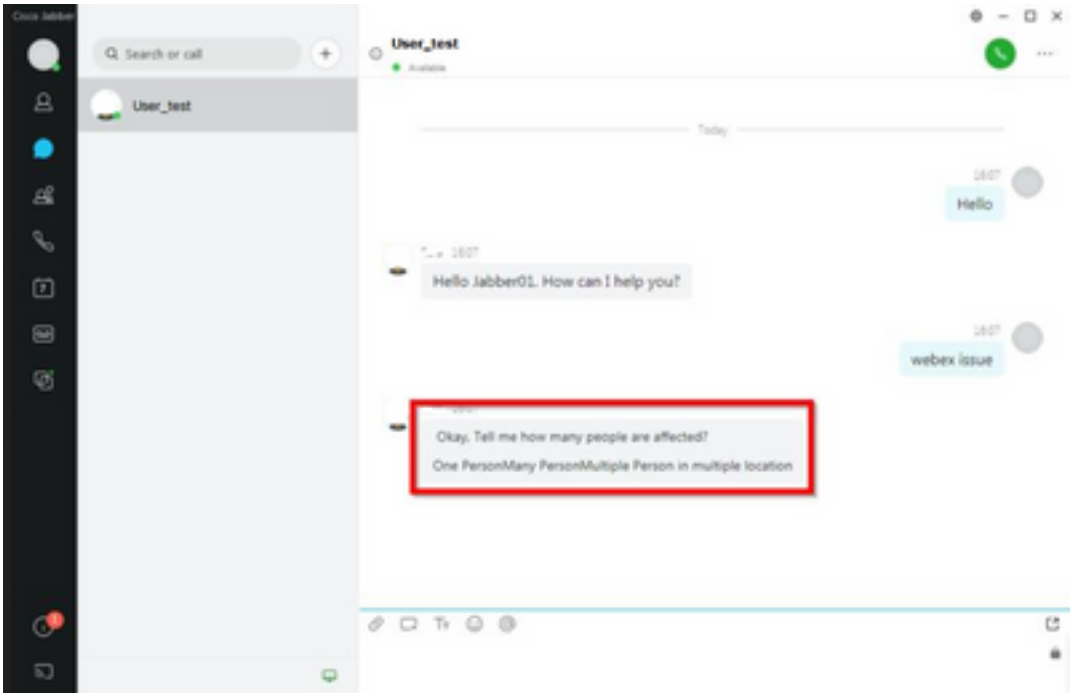
The information in this document is based on these software and hardware versions.

- Jabber version 12.9.X.
- Jabber version 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. If your network is live, ensure that you understand the potential impact of any command.

Problem

If the Jabber client version is 12.9.5, 14.0 or later, due to the vulnerabilities published last March 2022 (CVE-2020-3155), Jabber is now unable to render the content of the chatbots as they display the HTML content in the client interface.



That function makes Jabber vulnerable to attacks of man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then use a forged certificate to impersonate the endpoint. An exploit could allow the attacker to view presentation content shared on it, modify any content that is presented by the victim, or have access to call controls. This depends on the configuration of the endpoint.

Due to this vulnerability, the developers have introduced a security rule to allow several elements for Jabber in the HTML code tags to form the chatbot.

Before the vulnerability, there were no security checks for the bot message, but after the last vulnerability security change, the bot message is now checked by the new security mechanisms.

The security rule consists of the next allowed tags and style attributes.

Tags that are allowed.

```
{"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"}
```

Style attributes that are allowed.

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

Tags that are not allowed.

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

Solution

If the Cisco Jabber bot declaration has some or all of the non-allowed tags aforementioned, the solution consists in erase those tags from the HTML code. However, if they are needed for the bot to work, a configuration key is required.

To avoid any vulnerability at the same time, it is possible to use the classic chatbot created with the style attributes and allowed tags mentioned.

From the Jabber security fix, all other font styles or attributes outside the allowed list cannot be accepted. Therefore, you must change the attributes in the chatbot only to include those.

If you still require to use the chatbot normally, it means, with the unallowed tags, there is an HTML render option config key that can be added to the **jabber-config.xml** file (Jabber configuration file).

- hardening_xmpp_bot: set it to "FALSE" like in the example line.

Example: **<hardening_xmpp_bot>***FALSE***</hardening_xmpp_bot>**

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshoot information available for this configuration.

Related Information

- **Cisco Technical Support & Downloads**