Jabber에서 챗봇 콘텐츠를 렌더링할 수 없는 경우 문제 해결

목차

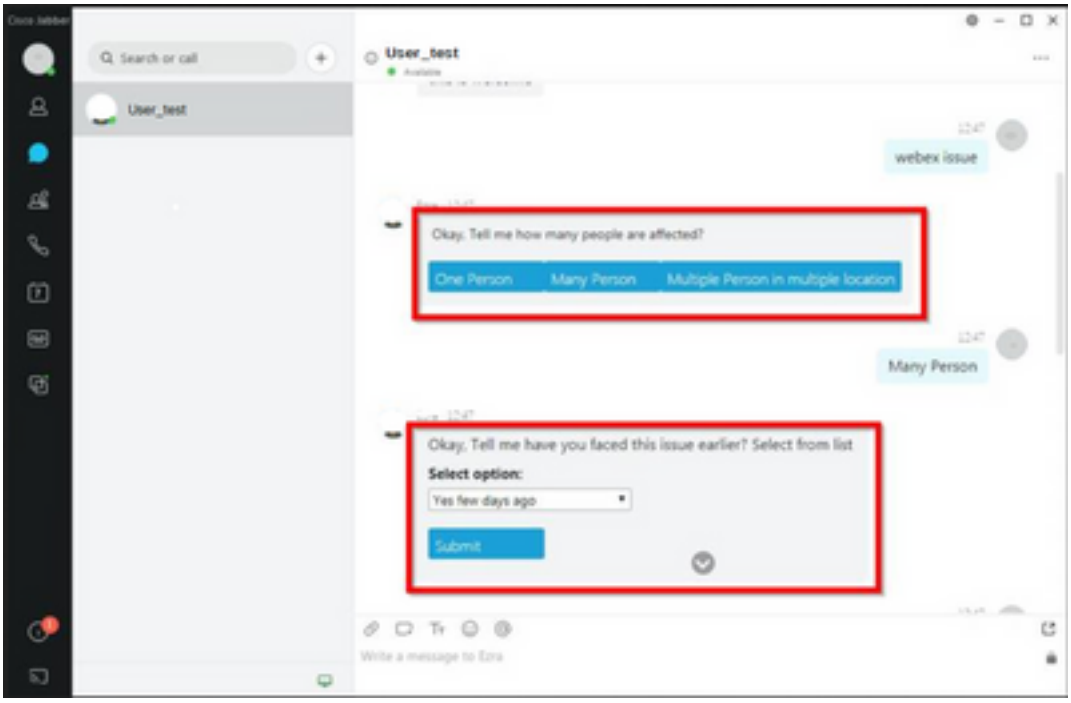
소개

이 문서에서는 Jabber 코드 수정 후 Cisco Jabber에서 챗봇 콘텐츠 렌더링 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

Jabber 클라이언트는 Cisco IM&P(Instant Messaging and Presence) 메시지 플랫폼 또는 Cisco Webex Messenger Server에서 대화형 대화형 봇을 구현하는 프레임워크 및 툴킷을 제공하는 SDK(Software Development Kit)로 개발된 Cisco Jabber Bot을 포함할 수 있습니다. 기본 Jabber 봇을 가져오도록 구성할 수 있는 특정 HTML(HyperText Markup Language) 태그가 있습니다.

Jabber 버전이 12.9.4 이전 버전이면 이미지에 표시된 것처럼 챗봇이 표시되고 Jabber에는 글꼴 코드에 설명된 모든 버튼과 옵션이 표시됩니다.



사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- Cisco Jabber
- Cisco Jabber Bot SDK

사용되는 구성 요소

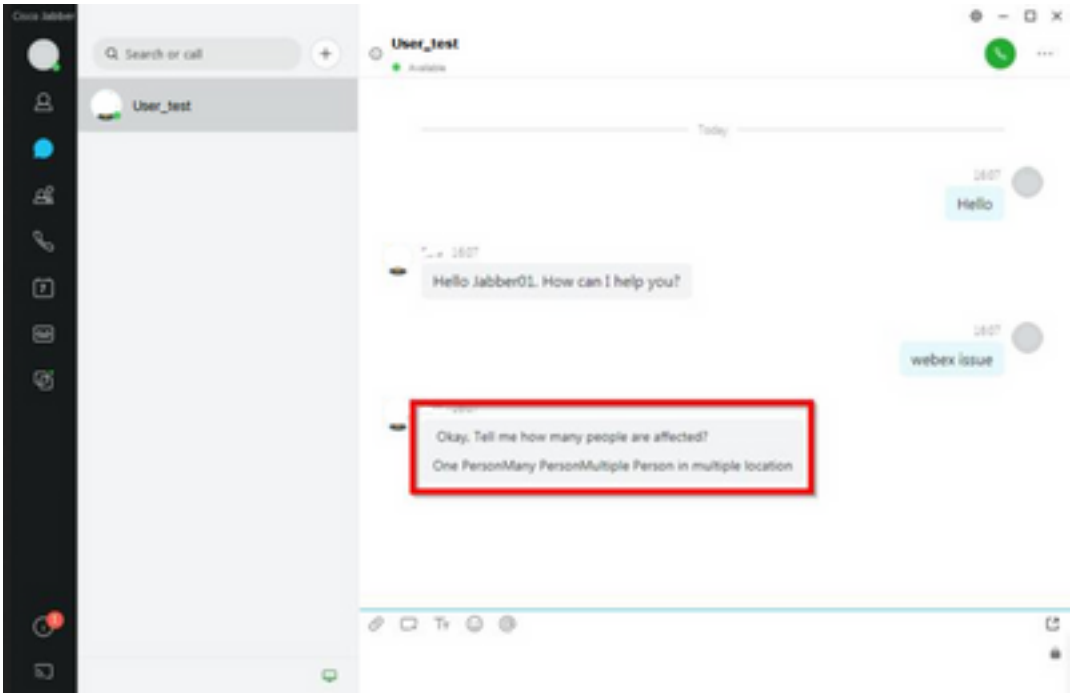
이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 12.9.X.
- Jabber 버전 14.X

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

Jabber 클라이언트 버전이 12.9.5, 14.0 또는 이후 버전인 경우, 2022년 3월에 게시된 취약성(CVE-2020-3155) 때문에 Jabber는 클라이언트 인터페이스에 HTML 콘텐츠를 표시하므로 이제 챗봇의 콘텐츠를 렌더링할 수 없습니다.



이 기능은 Jabber를 MITM(man in the middle) 기법의 공격에 취약하게 만들어 영향을 받는 클라이언트와 엔드포인트 간의 트래픽을 가로챈 다음 위조된 인증서를 사용하여 엔드포인트를 가장합니다. 공격자는 익스플로잇을 사용하여 해당 공격에서 공유된 프레젠테이션 콘텐츠를 보거나, 피해자가 제공한 콘텐츠를 수정하거나, 통화 제어에 액세스할 수 있습니다. 이는 엔드포인트의 컨피그레이션에 따라 달라집니다.

이러한 취약점으로 인해 개발자들은 HTML 코드 태그에 Jabber를 위한 여러 요소가 챗봇을 구성할 수 있도록 하는 보안 규칙을 도입했다.

취약성 이전에는 봇 메시지에 대한 보안 검사가 없었지만, 마지막 취약성 보안 변경 이후 봇 메시지는 이제 새로운 보안 메커니즘에 의해 검사됩니다.

보안 규칙은 다음으로 허용되는 태그 및 스타일 특성으로 구성됩니다.

허용되는 태그입니다.

```
{"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"}
```

허용되는 스타일 특성.

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

허용되지 않는 태그입니다.

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

솔루션

Cisco Jabber 봇 선언에 위에서 언급한 일부 또는 모든 허용되지 않는 태그가 있는 경우, 솔루션은 HTML 코드에서 해당 태그를 지우는 것으로 구성됩니다. 그러나 봇이 작동하는 데 필요한 경우 컨피그레이션 키가 필요합니다.

취약점을 동시에 방지하기 위해 스타일 속성과 허용되는 태그가 언급된 클래식 챗봇을 사용할 수 있습니다.

Jabber 보안 수정에서 허용되는 목록 밖의 다른 모든 글꼴 스타일 또는 특성을 수락할 수 없습니다. 따라서 챗봇의 속성만 포함하도록 변경해야 합니다.

챗봇을 정상적으로 사용해야 하는 경우 허용되지 않는 태그와 함께 jabber-config.xml 파일(Jabber 컨피그레이션 파일)에 추가할 수 있는 HTML 렌더링 옵션 컨피그레이션 키가 있음을 의미합니다.

- hardening_xmpp_bot: 예제 줄과 같이 "FALSE"로 설정합니다.

예: **<hardening_xmpp_bot>***FALSE***</hardening_xmpp_bot>**

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 구성에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.