SYNACKTIV
DIGITAL SECURITY

Stored Cross-Site Scripting (XSS) in Zimbra version 8.8.15_GA_4059 CVE-2022-41348

Security advisory

2023-04-07

Guillaume Jacques
Melvil Guillaume
Kévin Tellier

Vulnerabilities description

About Zimbra

Zimbra Collaboration Suite is a collaboration software suite, which includes an email server and a web client.

The issues

Synacktiv discovered a Stored Cross-Site Scripting (XSS) vulnerability in the Zimbra connect module.

Affected versions

At the time of writing, the version 8.8.15_GA_4059 (build 20210621055853) has proven to be affected. Other versions may also be concerned by this security issue.

Timeline

Date	Action
2021-10-29	Advisory sent to Zimbra
2022-10-10	Version 9.0.0 Patch 27 release and CVE-2022-41348 assigned
2023-04-07	Public release

Technical description and proof-of-concept

Stored Cross-Site Scripting (XSS)

The Zimbra web client application allows users to create Conversations. It was discovered that the name of the Conversation is not properly encoded once displayed to users. For instance, creating a new conversation with the following name would trigger the execution of *JavaScript* code: "*This is a new conversation meeting - *****"

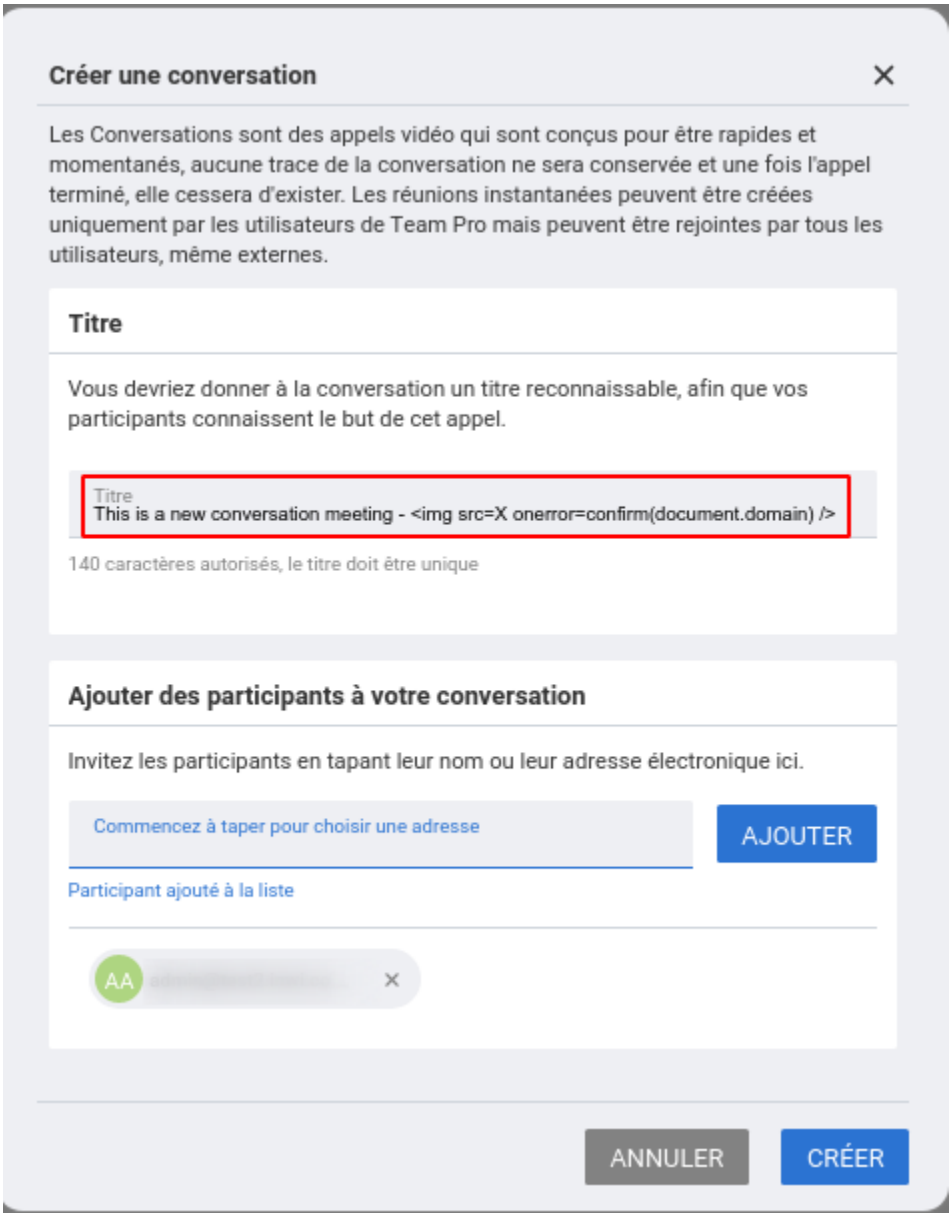

Illustration 1: Create a new conversation.

The invited user then receives a notification:

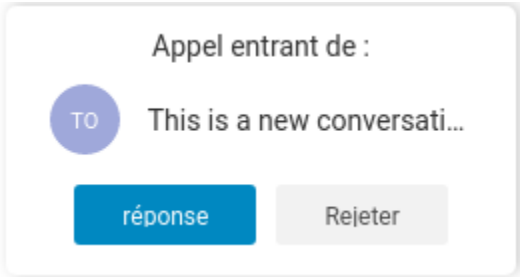

Illustration 2: Notification.

When the invited user chooses to join by clicking *answer* and *enter*, the *JavaScript* is executed:

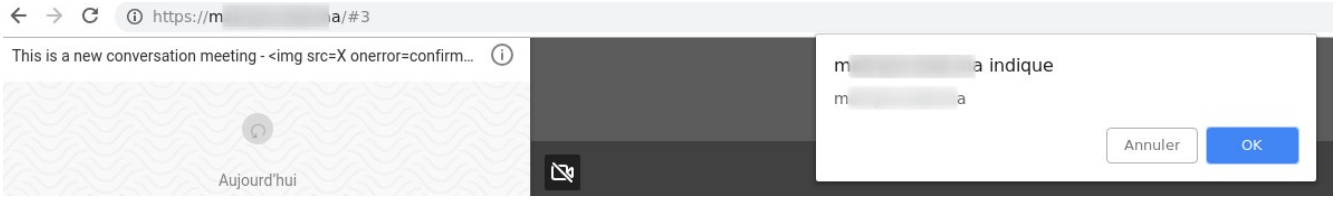

Illustration 3: Stored Cross-Site Scripting (XSS).