XSS when refreshing a checkboxradio with an HTML-like initial text label

Moderate **mgol** published **GHSA-h6gj-6jjq-h8g9** on Jul 15

Package

jquery-ui (npm)

Affected versions	Patched versions
<1.13.2	1.13.2

Description

Impact

Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. If you call `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities, they will erroneously get decoded. This can lead to potentially executing JavaScript code.

For example, starting with the following initial secure HTML:

```
<label>
        <input id="test-input">
        &lt;img src=x onerror="alert(1)"&gt;
</label>
```

and calling:

```
$( "#test-input" ).checkboxradio();
$( "#test-input" ).checkboxradio( "refresh" );
```

will turn the initial HTML into:

```
<label>
        <!-- some jQuery UI elements -->
```

```
        <input id="test-input">
        <img src=x onerror="alert(1)">
</label>
```

and the alert will get executed.

Patches

The bug has been patched in jQuery UI 1.13.2.

Workarounds

To remediate the issue, if you can change the initial HTML, you can wrap all the non-input contents of the `label` in a `span`:

```
<label>
        <input id="test-input">
        <span>&lt;img src=x onerror="alert(1)"&gt;</span>
</label>
```

References

https://blog.jqueryui.com/2022/07/jquery-ui-1-13-2-released/

For more information

If you have any questions or comments about this advisory, search for a relevant issue in the jQuery UI repo. If you don't find an answer, open a new issue.

Severity

Moderate

CVE ID

CVE-2022-31160

Weaknesses

No CWEs

Credits


Elkano