huntr

Stored XSS via Deserialization of Stylesheets in jgraph/drawio

2

✓ Valid Reported on Jun 6th 2022

Description

Diagram files can contain stylesheets which basically consist of key value pairs that influence the appearance of digram elements. When adding a stylesheet (`mxStylesheet` element) it is possible to execute JavaScript code when used in combination with the internal `include` element. Usually this would not be possible, because text content in stylesheets or its child elements would lead to an error when they are decoded in the application.
By using the `include` element and a data URI, this limitation can be bypassed. Adding a two element structure of nested `add` elements with the payload as the text content of the inner element allows executing any JavaScript code. The text content of the inner element is passed to an `eval` sink, which is enabled for `mxStylesheet` elements.

Proof of Concept

Save the following structure as `.drawio` file and open it in the web app:

```
<mxfile>
  <diagram id="aJXvI5cXjnzRwY48kwuR" name="Page-1">
    <mxGraphModel dx="719" dy="712" grid="1" gridSize="10" guides="1" toolt
      <mxStylesheet><include name="data:,&lt;mxStylesheet>&lt;add as=&quot
      <root>
        <mxCell id="0" />
        <mxCell id="1" parent="0" />
      </root>
    </mxGraphModel>
  </diagram>
</mxfile>
```

The JavaScript `alert` function will be executed

The JavaScript `alert` function will be executed.
Note: The desktop application is not affected. The deployment on app.diagrams.net is also not affected because it uses a custom CSP.

Impact

Stored XSS via diagram files which allows stealing of user secrets like authentication tokens. Further malicious actions might be possible depending on the context where the drawio library is used.

Occurrences

JS app.min.js L2258

Unfortunately this is located in the minified sources. Responsible is the following setting: `mxStylesheetCodec.allowEval = !0;` In the formatted sources this can be found on line 32826.

CVE
CVE-2022-2015
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.1)

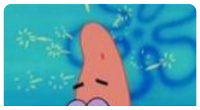
Registry
Other

Affected Version
<= 19.0.1

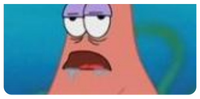
Visibility
Public

Status
Fixed

Found by



Tobias S. Fink
@7085



legend ⌄

This report was seen 684 times.

We are processing your report and will contact the **jgraph/drawio** team within 24 hours. 6 months ago

David Benson validated this vulnerability 6 months ago

Tobias S. Fink has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

David Benson marked this as fixed in **19.0.2** with commit **3d3f81** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

app.min.js#L2258 has been validated ✓

Sign in to join this conversation

2022 © 418sec

huntr	part of 418sec
home	company
hacktivity	about

Chat with us

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us