

New issue

[Jump to bottom](#)

User can inject JavaScript code into the text node which can cause security issues(Cross-Site Scripting) #772

✓ Closed

1 of 2 tasks

GowriAradhya opened this issue on Aug 5 · 0 comments

GowriAradhya commented on Aug 5

What are the steps to reproduce?

Drag Dashboard Text Node and inject node into the Node-red workspace . Click on Edit text node and add value format value as `{{constructor.constructor('alert(document.cookie')}())}}`.

What happens?

Malicious script code can be injected permanently into the Node-red. Using injected code, an user could, for example, steal Node Red identifiers of any other sensitive information.

What do you expect to happen?

when Data in JavaScript format is injected to text node output must be converted to string .

Please tell us about your environment:

[x] Node-RED-Dashboard version: 3.1.2

[x] Node-RED version: 2.1.4

[x] node.js version: 14.18.2

☐ npm version:

☒ Platform/OS: docker

[x] Browser: Chrome

 dceejay closed this as completed in [9305d1a](#) on Sep 9

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

