New issue

Jump to bottom

[Bug Report] [Component] [table-column] table-column 中对于 属性 show-overflow-tooltip 处理存在问题 可以导致 XSS #6514

Closed **Esonhugh** opened this issue on Mar 10 · 8 comments · Fixed by #6520

Assignees 

Labels Component::Table Level::P0 Project::Bug

Esonhugh commented on Mar 10

Bug Type: `Component`

Environment

- Vue Version: `3.2.13`
- Element Plus Version: `2.0.5`
- Browser / OS: `UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36`
- Build Tool: `Vue CLI`

Reproduction

Related Component

- `el-table-column`

Reproduction Link

Github Repo

Steps to reproduce

按照 复现项目的 readme 进行构建
访问 serve
在 含有 payload 的 address 的列处中划过光标 就可以触发 js 运行导致 xss

What is Expected?

渲染img或者不渲染都可以 但不可以执行 JavaScript

What is actually happening?

渲染文本内容为 html 并且执行 JavaScript 脚本

Additional comments

elementui plus 是一个大仓库导致有许许多多的前端项目依赖其而构建
show-overflow-tooltip 已经可以通过 github 代码搜索 找到相关项目 并且其中包含一些部分后台管理项目
建议通知开发者 更新项目与修复该问题
此外文档中建议添加相关 安全警告

其他相关信息:
asjdf/element-table-xss-test#1

Reporter:
@Esonhugh
@asjdf

msidolphin added Project::Bug **Component::Table** **Level::P0** labels on Mar 10

msidolphin self-assigned this on Mar 10

Esonhugh commented on Mar 10 — Author

此外提一个小问题： 请问我可以为此提 CVE 编号或者 CNVD 编码嘛

jw-foss commented on Mar 10 — Member

> 此外提一个小问题： 请问我可以为此提 CVE 编号或者 CNVD 编码嘛

这里是指?

Esonhugh commented on Mar 10 — Author

> 此外提一个小问题： 请问我可以为此提 CVE 编号或者 CNVD 编码嘛
>
> 这里是指?

为这个可以引发 xss 安全问题的 "bug" or 漏洞
申请通用漏洞编号

👍 2

jw-foss commented on Mar 10 — Member

可以，如果你想做的话

Esonhugh commented on Mar 10 — Author

> 可以，如果你想做的话

感谢您的支持 element plus 是个很棒的框架。

❤️ 2

jw-foss commented on Mar 10 — Member

@Esonhugh 感谢告知这个问题，我们会立即修复。

msidolphin mentioned this issue on Mar 10

fix(components): [el-table] escape special html characters #6520

Merged

3 tasks

jw-foss closed this as completed in #6520 on Mar 11

Esonhugh commented on Mar 11 — Author

> @Esonhugh 感谢告知这个问题，我们会立即修复。

Nice Fix.

顺带说一句, 也算是个人的一个小建议. 我在报送这个安全性问题, 尝试寻找项目负责人和维护人的时候 遇到了找不到安全类 issue privately 报送的方法. 例如: JeremyWuuuuu 大佬的邮箱 我并没有在 github profile 这种地方找到, 不过 sxzz 大佬给予了我一些帮助

或许可以试试开启 github 的 这个功能? Github Security Advisories

👀 1

github-actions bot commented on Apr 10

This issue has been automatically locked since there has not been any recent activity after it was closed. Please open a new issue for related bugs.

此 issue 已被自动锁定，因为关闭后没有任何近期活动。如果有相关 bug，请重新创建一个新 issue。

github-actions bot locked and limited conversation to collaborators on Apr 10

Assignees

msidolphin

Labels

Component::Table Level::P0 Project::Bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

fix(components): [el-table] escape special html characters
element-plus/element-plus

3 participants