hapifhir / **hapi-fhir** Public

Code Issues 627 Pull requests 115 Actions Projects Wiki ···

New issue

Jump to bottom

XSS Vulnerability in Testpage Overlay #2026

Closed **jamesagnew** opened this issue on Aug 8, 2020 · 0 comments · Fixed by #2027

jamesagnew commented on Aug 8, 2020 Collaborator

Thanks to Will Davison of NCC Group (Manchester UK) for disclosing this vulnerability.

Text of disclosure follows:

> Evidence – Reflected XSS:
>
> It was possible to send a GET request to the HAPI FHIR Web Application such that any included malicious code would be executed in the victim's browser. This could be used to craft a phishing link, for example.
>
> By URL-encoding twice, it was possible to bypass any sanitisation on URL-parameters which were reflected In the page body.
> The following double URL-encoded payload was used to display an alert box:
>
> `<script>alert('XSS')</script>`
>
> URL-encoding once transforms the string into:
> `%3cscript%3ealert%28'XSS'%29%3c%2fscript%3e`
> URL-encoding once more gives us our final payload of:
> `%253cscript%253ealert%2528%27XSS%27%2529%253c%252fscript%253e`
>
> Being used to craft a PoC Link such as:
> http://localhost:8080/hapi-fhir-jpaserver/read?serverId=home&pretty=true&resource=Account&id=0e1dt4%253cscript%253ealert%2528%27XSS%27%2529%253c%252fscript%253efnvk4&vid=%20
>
> In the above example, the vulnerable parameter is "id" but this should also work for vid and account. It's likely that this issue is present in a few places, but I have not exhaustively tested. I would recommend reviewing the code in order to ensure both input sanitisation and output encoding are consistent across the application.
> OWASP's Cheat Sheet series may be of some use here: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md

This vulnerability affects only users of the "Testpage Overlay" HAPI FHIR module. Maven coordinates for this module are:
groupID: ca.uhn.hapi.fhir
artifactID: hapi-fhir-testpage-overlay

Affected versions are any versions 5.0.0 and below. This issue is resolved in version 5.1.0

Analysis:
Users of the HAPI FHIR Testpage Overlay can use a specially crafted URL to exploit an XSS vulnerability in this module, allowing arbitrary JavaScript to be executed in the user's browser. The impact of this vulnerability is believed to be low, as this module is intended for testing and not believed to be widely used for any production purposes. Nonetheless, we recommend all users of the affected module upgrade immediately.

A complete audit of the affected codebase has been completed in order to detect and resolve any similar issues.

jamesagnew mentioned this issue on Aug 8, 2020

Fix TestpageOverlay XSS Vulnerability #2027

Merged

jamesagnew closed this as completed in #2027 on Aug 9, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix TestpageOverlay XSS Vulnerability
hapifhir/hapi-fhir

1 participant