New issue

Jump to bottom

[CVE-2021-26722] Reflected Cross-Site Scripting in search bar. #341

Closed **renniepak** opened this issue on Feb 5, 2021 · 3 comments

renniepak commented on Feb 5, 2021

Hi!

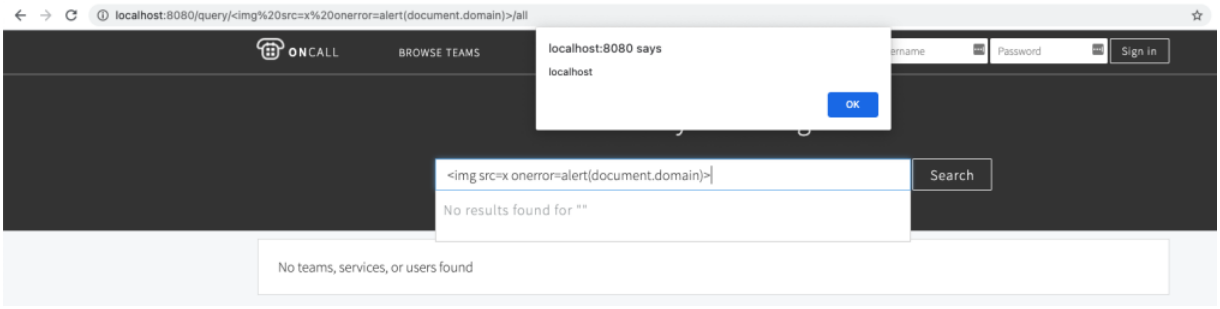
I've found a reflected cross-site scripting vulnerability in Oncall's search bar. I've reported this issue to the LinkedIn Information Security Response Center back in September 2020 but Oncall still seems vulnerable to this date. Therefore I decided to report it here.

Reproduction

1. Navigate to `http://[OnCallHost]/query/%3Cimg%20src=x%20onerror=alert(document.domain)%3E/all`
2. Click on the search bar where it now says `<img src=x onerror=alert(document.domain)>`

Result

By clicking the search bar, a search will be done to the search API endpoint. Because nothing can be found a `No results found for "<img src="x" onerror="alert(document.domain)">"` message will be shown. Because this message includes the search query and lacks the proper HTML output encoding, the query is interpreted as HTML/JS and an alert containing the `document.domain` is shown.



Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:

- Steal the user's credentials by altering the working of the displayed login form.
- Perform any action within the application that the user can perform.
- View any information that the user is able to view.
- Modify any information that the user is able to modify.

Mitigation

In general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

- **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- **Encode data on output.** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- **Content Security Policy.** As a last line of defense, you could use a (default) Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

renniepak changed the title ~~Reflected Cross-Site Scripting in search bar.~~ **Reflected Cross-Site Scripting in search bar.** on Feb 5, 2021

diegocepedaw commented on Feb 5, 2021 Contributor

Hi **@renniepak**, thanks for bringing this to our attention. Unfortunately, we weren't previously informed of the issue by the Information Security Response Center but now that we are aware of this problem we will be addressing it with the highest priority.

1

renniepak commented on Feb 5, 2021 Author

Hi **@diegocepedaw**,

Thanks for the quick response.
I've requested a CVE for this issue and got the confirmation that it will be assigned `CVE-2021-26722`.

If there are any questions, I'm happy to help.

renniepak changed the title ~~Reflected Cross-Site Scripting in search bar.~~ **[CVE-2021-26722] Reflected Cross-Site Scripting in search bar.** on Feb 5, 2021

diegocepedaw mentioned this issue on Feb 5, 2021

prevent potential XSS from searchbar results #342

Merged

diegocepedaw commented on Feb 5, 2021 Contributor

Opened PR #342 to address the issue and will be requesting a further security review from our security team to make sure there are no other similar issues.

1

diegocepedaw closed this as completed on Feb 5, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants