uclahs-secops / **security-research** Public

<> **Code** ⊙ Issues Pull requests ▷ Actions Projects Security Insights

main ▾ security-research / reports / 20221011-recap-xss /

mednet-mtaggart Add CVE-2022-42715 … on Oct 11 **History**

..	
img	2 months ago
README.md	2 months ago

README.md

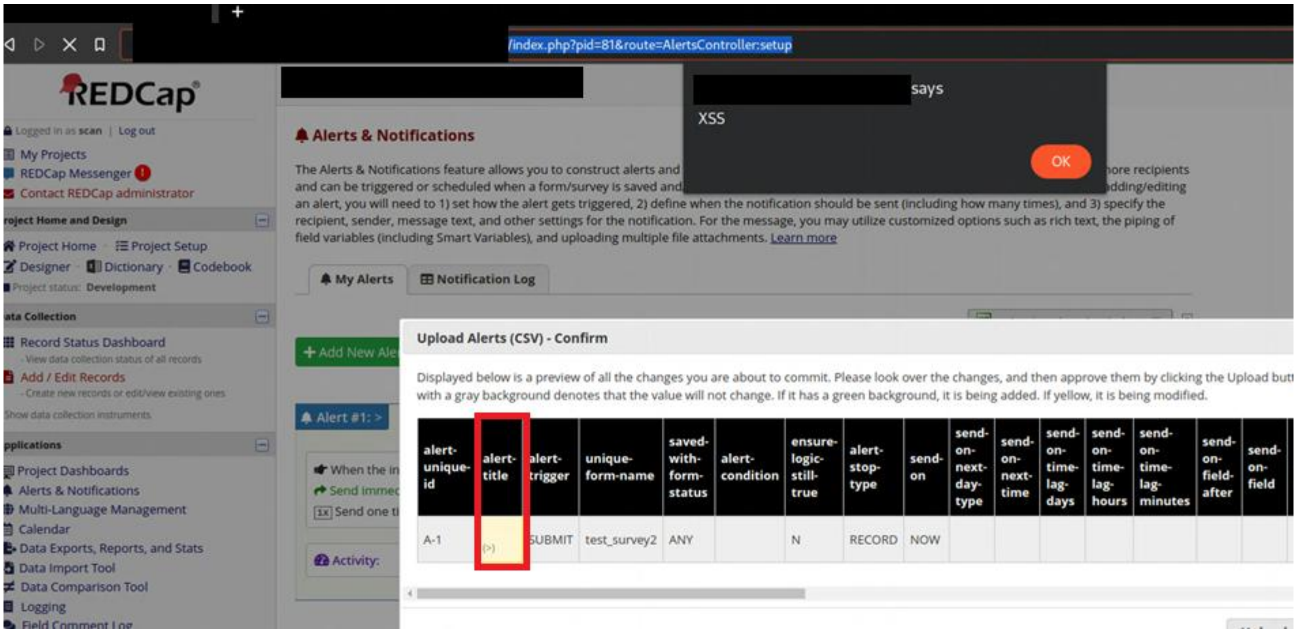
CVE-2022-42715: Reflected Cross-Site Scripting in REDCap Versions <12.4.18, 12.5.11

Issue Summary

A reflected cross-site scripting vulnerability exists in Vanderbilt University's Project REDCap survey management tool, leading to arbitrary JavaScript execution in a user's browser.

The import function in the Alerts & Notifications section of REDCap version 12.4.12 is vulnerable to DOM-based cross-site scripting. By uploading a maliciously crafted CSV to the portal, the alert fields are interpreted without XSS checks during review, leading to JavaScript execution.

Proof of Exploitation



[redacted]/index.php?pid=81&route=AlertsController:setup
REDCap
Logged in as scan | Log out
My Projects
REDCap Messenger
Contact REDCap administrator
roject Home and Design
Project Home · Project Setup
Designer · Dictionary · Codebook
Project status: Development
ata Collection
Record Status Dashboard
- View data collection status of all records
Add / Edit Records
- Create new records or edit/view existing ones
Show data collection instruments
pplications
Project Dashboards
Alerts & Notifications
Multi-Language Management
Calendar
Data Exports, Reports, and Stats
Data Import Tool
Data Comparison Tool
Logging
Field Comment Log
My Alerts
Notification Log
+ Add New Ale
Alert #1: >
When the in
Send immec
1x Send one ti
Activity:

[redacted]

[redacted] says

XSS

OK

Alerts & Notifications

The Alerts & Notifications feature allows you to construct alerts and … ore recipients and can be triggered or scheduled when a form/survey is saved and … dding/editing an alert, you will need to 1) set how the alert gets triggered, 2) define when the notification should be sent (including how many times), and 3) specify the recipient, sender, message text, and other settings for the notification. For the message, you may utilize customized options such as rich text, the piping of field variables (including Smart Variables), and uploading multiple file attachments. Learn more

Upload Alerts (CSV) - Confirm

Displayed below is a preview of all the changes you are about to commit. Please look over the changes, and then approve them by clicking the Upload butt with a gray background denotes that the value will not change. If it has a green background, it is being added. If yellow, it is being modified.

alert-unique-id	alert-title	alert-trigger	unique-form-name	saved-with-form-status	alert-condition	ensure-logic-still-true	alert-stop-type	send-on	send-on-next-day-type	send-on-next-time	send-on-time-lag-days	send-on-time-lag-hours	send-on-time-lag-minutes	send-on-field-after	send-on-field
A-1	(>)	SUBMIT	test_survey2	ANY		N	RECORD	NOW							

After uploading the malicious CSV, arbitrary JavaScript executes in the user's browser.

Issue Impact

Although exploitation of this vulnerability would require a user to upload a maliciously-crafted CSV, if one were provided to the user and uploaded without scrutiny, the user could be coerced to disclose credentials, download malware, or other common JavaScript-based techniques used by attackers.

Discovery/Disclosure Timeline

- 9/21/22: Vulnerability discovered
- 9/23/22: Vulnerability reported to REDCap
- Ticket #134640 opened by REDCap
- 10/3/22: Patch provided by REDCap
- 10/4/22: CVE Requested
- 10/9/22: CVE-2022-42715 Assigned
- 10/11/22: Writeup Published

References

- REDCap Changelog