REDCap Flex Upgrade Changelog – September 19 2024 Upgrade (v.14.5.9 → v.14.5.13)

Version 14.5.13

- Critical security fix: A Remote Code Execution vulnerability was found in which a malicious user who is logged in could potentially exploit it by manipulating an HTTP request to a specific External Module Framework endpoint. If successfully exploited, this could allow the attacker to remotely execute arbitrary code on the REDCap server. This vulnerability exists in REDCap 11.0.0 and higher.
- Critical security fix: A Remote Code Execution vulnerability was found in which a malicious user who is logged in could potentially exploit it by manipulating an HTTP request to the Data Import Tool page while uploading a specially-crafted CDISC ODM XML file. If successfully exploited, this could allow the attacker to remotely execute arbitrary code on the REDCap server. This vulnerability exists in REDCap 6.12.0 and higher.
- Major security fix: A Cross-Site Request Forgery (CSRF) Bypass vulnerability was found in which a malicious user could potentially exploit it by manipulating an HTTP request to any URL in the system by tricking an authenticated user to click a specially-crafted link that could bypass the CSRF check and submit information (including changing REDCap system configuration values) on behalf of the user or admin. This vulnerability exists in REDCap 13.4.0 and higher.
- Major security fix: A Local File Inclusion (LFI) vulnerability was discovered in which a malicious user could potentially exploit it by setting the path of the hook function file on the General Configuration page to a value containing specific characters in order to bypass the check that ensures that the file path points to a PHP file. The user must have "Modify system configuration pages" administrator privileges in order to exploit this. This bug affects all known REDCap versions.
- Major security fix: A Stored XSS (Cross-site Scripting) vulnerability was discovered in which a malicious user could potentially exploit it by inserting custom HTML and JavaScript in a specially crafted way that can be exploited on the following pages: Alerts & Notifications, Stats & Charts, and the main REDCap Home Page. This vulnerability can only be exploited by authenticated users. Bug exists in all REDCap versions.
- Medium security fix: A Blind SQL Injection vulnerability was found on certain Clinical Data Mart (CDM) related pages, in which a malicious user could potentially exploit it and execute arbitrary SQL commands on the database by manipulating an HTTP request in a specially-crafted way. The user must have "Access to all projects and data with maximum user privileges" administrator privileges in order to exploit this. This bug affects all known REDCap versions.
- Medium security fix: A Blind SQL Injection vulnerability was found on several Control Center pages, in which a malicious user who has co-opted a REDCap admin account could potentially exploit it and execute arbitrary SQL commands on the database by manipulating an HTTP request in a specially-crafted way. The user must have "Modify system configuration pages" administrator privileges in order to exploit this. This bug affects all known REDCap versions.

- Medium security fix: A Blind SQL Injection vulnerability was found on the Edit Project Settings page, in which a malicious user could potentially exploit it and execute arbitrary SQL commands on the database by manipulating an HTTP request in a specially-crafted way. The user must have "Access to all projects and data with maximum user privileges" administrator privileges in order to exploit this. This bug affects all known REDCap versions.
- Medium security fix: A Blind SQL Injection vulnerability was found on the Online Designer page, in which a malicious user could potentially exploit it and execute arbitrary SQL commands on the database by manipulating an HTTP request in a specially-crafted way. The user must be logged in to REDCap in order to exploit this. This bug affects all known REDCap versions.
- Medium security fix: A Blind SQL Injection vulnerability was found on the Send-It upload page, in which a malicious user could potentially exploit it and execute arbitrary SQL commands on the database by manipulating an HTTP request in a specially-crafted way. The user must be logged in to REDCap in order to exploit this. This bug affects all known REDCap versions.

Version 14.5.12

- Major bug fix: In rare cases where radio field choices are being piped on a form or survey, the page might mistakenly never fully load due to a JavaScript error.
- Bug fix: Mapped fields in projects marked as both CDP and CDM were not displaying correctly in the CDIS Mapping Helper tool.
- Bug fix: Some text inside red boxes throughout REDCap would mistakenly appear in a much lighter red color than intended.
- Bug fix: When users are deleting multiple fields in the Online Designer, in some rare cases a race condition might occur that scrambles the field order and results in fields being suddenly in the wrong location.
- Bug fix: When using the MyCap "App Design" page, a JavaScript error would occur when clicking the "Publish" button. This issue prevents a success message box from appearing on the page.

Version 14.5.11

- Major bug fix: When the e-Consent Framework has been set up but then later disabled for a given survey, a PDF Snapshot would mistakenly still get saved to the File Repository and/or specified File Upload field whenever a participant completes the survey. (Ticket #239030)
- Bug fix: MyCap participants would mistakenly not receive any push notifications upon a user (e.g., study coordinator) sending them an announcement via the MyCap messaging interface in the project.
- Bug fix: Radio fields with the action tags READONLY and DEFAULT or SETVALUE would mistakenly not pipe correctly on the page.
- Bug fix: Some unwanted text would mistakenly be displayed at the bottom of the Edit Project Settings page. (Ticket #238981)
- Bug fix: When opening the "Edit Branching Logic" dialog via the Quick Modify Fields popup on the Online Designer, the branching logic text box in the dialog would mistakenly retain the

previous value entered by the user while on that same current page. The text box's value should be cleared out each time the dialog is opened. (Ticket #238833)

- Bug fix: When performing a data import on the Data Import Tool page, in some rare situations, the import process might mistakenly fail due to a fatal PHP error when using PHP 8. (Ticket #238912)
- Bug fix: When using "OpenID Connect" or "OpenID Connect & Table-based" authentication, and a user logs out of REDCap and then later logs back in again, the login process might mistakenly fail silently when re-logging again. (Ticket #237124)
- Bug fix: When using Multi-Language Management in a project with MyCap enabled, the language ISO codes displayed for MyCap in the "Add New Language" dialog on the MLM setup page were incorrect for many of the languages listed. Those ISO codes have been corrected.
- Bug fix: When viewing a report that has report logic that includes checkbox fields that reference Missing Data Codes (e.g., [my_checkbox(NA)] = "1"), the report might mistakenly not return items/data that should be returned, specifically when displaying data for repeating instruments.

Version 14.5.10

- Bug fix: Alerts with conditional logic containing datediff() with "today" or "now" as a parameter might mistakenly get triggered multiple times by the cron job, thus resulting in duplicate alerts being sent. This behavior appears to be sporadic and occurs very seldom for most installations. (Ticket #237341)
- Bug fix: Horizontally-aligned enhanced radios/checkboxes on surveys that do not have a question number column would mistakenly not be spaced out consistently between each choice on a given horizontal line. Note: This fix is slightly different from a similar one from last week, which did not get completely fixed.
- Bug fix: If a user has received a confirmation link via email for registering a new email address with their REDCap account, and then the REDCap server is upgraded to a new REDCap version after the email is received, the link in the email would mistakenly redirect to the wrong place in the new version, thus preventing the user from being able to complete the email registration process. (Ticket #238619)
- Bug fix: In certain specific situations, logged events related to clicking Project Bookmarks might mistakenly be displayed on the Logging page when filtering by a specific record in the project. (Ticket #238547)
- Bug fix: In some cases when inline PDFs are attached to Descriptive fields, and a user downloads the PDF of the instrument, if the iMagick PHP extension is installed on the web server, the first page of the inline PDF might mistakenly get truncated in the resulting REDCap-generated PDF of the instrument.
- Bug fix: In some cases when inline PDFs are used as consent forms in the e-Consent Framework, and a user downloads the PDF of the instrument, if the iMagick PHP extension is installed on the web server, there would mistakenly be a blank page following the inline PDFs in the resulting REDCap-generated PDF of the instrument. (Ticket #237921)
- Bug fix: Several missing LOINC codes were added to the CDIS mapping features. Additionally, several Clinical Notes types were missing and not mappable, specifically pathology study, diagnostic imaging study, and laboratory report.

- Bug fix: The CSV file download option for the Choices Editor inside the Edit Field dialog for multiple choice fields in the Online Designer would mistakenly not do anything. (Ticket #238818)
- Bug fix: When a Data Entry Trigger is triggered on a data entry form for a record in a Data Access Group, the unique DAG name would mistakenly not get sent in the request to the Data Entry Trigger URL. Note: This issue does not occur on survey pages, and it also does not occur on data entry forms when a record is being assigned to a DAG while also being created there on the form. (Ticket #238727)
- Bug fix: When comparing two records in the Data Comparison Tool, the coded values of multiple choice fields would be mistakenly wrapped in escaped HTML italic tags, which would cause the tags to be visible (rather than interpreted) on the page. Bug emerged in REDCap 14.0.14 LTS and 14.2.1 Standard. (Ticket #238437)
- Bug fix: When copying a project via the "Copy the Project" page for a project that contains a repeating survey with a repeating Automated Survey Invitation, the ASI's recurrence settings (e.g., "How many times to send it") would mistakenly not get copied into the new project. Bug emerged in REDCap 12.5.0. (Ticket #238218)
- Bug fix: When downloading a PDF of "All forms/surveys with saved data" or "All forms/surveys with saved data (compact)" when some instruments contain embedded fields, some of the embedded fields might mistakenly not get converted into data values or underscores (if they have no value) in the resulting PDF. (Ticket #238683)
- Bug fix: When modifying a PDF Snapshot, some of the snapshot settings (specifically the checkbox options) might mistakenly not get saved successfully after being changed, and no error would be displayed to notify the user that their desired settings were not saved. This issue only affects web servers running PHP 7.3 or 7.4. (Ticket #236067)
- Bug fix: When participants are taking a survey that contains fields with the @HIDDEN-SURVEY action tag, in which the participant is using a non-standard web browser, the fields might mistakenly be displayed instead of hidden on the survey page. (Ticket #238129)
- Bug fix: When selecting instruments for the scope of a PDF Snapshot, the "Update" and "Cancel" buttons may disappear when scrolling downward when many instruments exist in the box, thus possibly causing confusion with regard to how to save one's selected instruments. To fix this, the buttons now float at the top of the box regardless of scrolling. (Ticket #238698)
- Bug fix: When the Confirmation Email option has been enabled, specifically with the "Include PDF of completed survey as attachment" checkbox checked, for a survey that has the e-Consent Framework enabled, the PDF attached to the email received by the participant would mistakenly contain the record name of the participant's record in the filename of the PDF. The record name should not be included in the PDF filename for PDFs received by participants. (Ticket #223899)
- Bug fix: When the Top Usage Report page displays a row that is a "Project" type, the project link displayed in that row would mistakenly be an invalid URL if the project title ends with text enclosed in parentheses. (Ticket #238523)
- Bug fix: When using Clinical Data Pull for CDIS, in the "launch from EHR" context of a CDIS project, events were not logged properly when a patient was added to a project. This improper logging prevented the record list cache in REDCap from rebuilding correctly, leading to issues when saving records in projects with auto-incrementing record IDs. (Ticket #234550)

Bug fix: When using certain screen readers, such as JAWS, the individual options of drop-down fields might mistakenly not be able to be read by the screen reader. (Ticket #237629)