# REDCap Flex Upgrade Changelog – June and July 2024 Upgrade (v. 14.0.24 → v.14.0.33)

## Version 14.0.33

- Medium 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 into the contents of a file that is uploaded via the API and then downloaded via the API using various file import/export API methods. This vulnerability can be exploited only by users that possess a REDCap API token. Bug exists in all REDCap versions.
- Medium security fixes: Several access control vulnerabilities were discovered in REDCap Messenger in which a malicious user could potentially exploit them by sending specially crafted HTTP requests that would allow them to perform the following actions: read and export any conversation in the system, add a message to any conversation, add themselves as a conversation leader on any conversation, upload a file to any conversation, and export a list of all users of a conversation. Bug exists in REDCap 7.4.0 and later.
- 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 into any user input that is then output on a page in REDCap (e.g., field labels, survey instructions, data displayed on a report). This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all 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 into the record name when creating a new Calendar event on the Calendar page, specifically in the Calendar popup. This vulnerability can be exploited by authenticated users only. Bug exists in all REDCap versions.
- Bug fix: A fatal PHP 8 error might occur in a specific situation when a participant is taking an adaptive or auto-scoring instrument (i.e., a PROMIS assessment) from the REDCap Shared Library. (Ticket #234346)
- Bug fix: Fixed several PHP 8 related errors. (Ticket #233266)
- Bug fix: Some PHP errors might mistakenly occur when using Azure Blob Storage when performing certain tasks. (Ticket #234248)
- Bug fix: When a field is embedded in a checkbox or radio field's choice label while that checkbox/radio field is also piped somewhere on the current page, the value of the embedded field might mistakenly not get saved correctly when a user modifies it and saves the page. (Ticket #233917b)
- Bug fix: When a participant is attempting to enter data for a biomedical ontology field while on a survey page, the ontology field would not function correctly and would not fetch any values from the BioPortal web service. This issue occurs on survey pages only. Bug emerged in the previous version.

- Bug fix: When taking a survey, malicious survey participants could possibly alter the "start time" of their response by carefully manipulating hidden elements on the first page of a survey. Note: This does not affect the security of the survey but might affect data quality.
- Bug fix: When using Clinical Data Pull for CDIS, a JavaScript error might occur when adding a patient to a project in the "Launch from EHR" process, thus preventing the patient from being added. (Ticket #234249)
- Bug fix: When using Twilio or Mosio, it would mistakenly not send SMS messages to U.S. phone numbers with certain newer area codes, including 787 and 939. (Ticket #234300)
- Bug fix: When viewing a public report that contains the record ID field, if the Secondary Unique Field has been defined in the project and has also been tagged as an identifier field, then the public report would mistakenly not display and would output an error message even if the setting "Display the value of the Secondary Unique Field next to each record name displayed?" is disabled. (Ticket #234403)

## Version 14.0.32

- Bug fix: A rare issue might occur when non-checkbox fields from a repeating instrument or repeating event are referenced inside branching logic or calculated fields. (Ticket #233509)
- Bug fix: Embedded fields might mistakenly get hidden when also piped on the same form under very specific circumstances. (Ticket #233917)
- Bug fix: Fixed several PHP 8 related errors. (Ticket #233266)
- Bug fix: If the Send-It feature has been disabled at the system level, the "Share" dialog for files stored in the File Repository would mistakenly still display an option to share the file using Send-It. (Ticket #233493)
- Bug fix: In some very specific situations, a @CALCTEXT action tag that contains a plus sign (" ") character might produce an unexpected result. (Ticket #233189)
- Bug fix: In specific scenarios when viewing MDY or DMY formatted date fields on a report, the date values might mistakenly appear mangled on the page. (Ticket #211780)
- Bug fix: Resolved an issue with the link to the Mapping Helper in the CDIS panel menu. (Ticket #226611)
- Bug fix: The documentation for the "Export Users" API method would mistakenly make mention of the "Read Only" rights for the "User Rights" privilege when the "Read Only" option for the "User Rights" privilege does not exist in the current LTS but in the latest Standard Release. This text has been edited to remove reference to that feature that does not exist in LTS yet. (Ticket #233936)
- Bug fix: The month and year drop-downs inside the datetime pickers for the "start time" and "end time" filters on the Logging page would not work and would mistakenly not change the start/end times after a new option was selected for those drop-downs. (Ticket #233815)
- Bug fix: Under certain circumstances where quote characters are next to equal signs, CALCTEXT expressions might not be parsed correctly and thus might produce a JavaScript error. (Ticket #233927)
- Bug fix: When a user has "read-only" data viewing access to an instrument that contains a biomedical ontology field, the ontology field would appear to be editable on the page, despite

the fact that the user is not able to submit the page or modify the field's saved value. (Ticket #233940)

- Bug fix: When clicking the "Add new template" button on the Project Template page in the Control Center, the popup might time out and never be displayed if tens of thousands of projects exist in the system. To prevent this, an auto-complete drop-down will replace the regular drop-down when more than 5000 projects exist. (Ticket #233451)
- Bug fix: When creating a new alert on the Alerts & Notifications page, in which the Twilio, Mosio, and Sendgrid services for alerts have been disabled at the system level, the "Email to send email-failure errors" setting would mistakenly not be displayed after clicking the "Show more options" link in the "Create new alert" dialog. (Ticket #233629)
- Bug fix: When exporting the Participant List via CSV on the Participant List page, some columns might mistakenly have the wrong header labels in the CSV file. (Ticket #233958)
- Bug fix: When the HTML tags "iframe" or "embed" are added to any user input that is then output on a page in REDCap (e.g., field labels, survey instructions), any text or tags that occur after the iframe/embed tags would mistakenly be removed along with the iframe/embed tags themselves, thus truncating the text. Note: iframe/embed tags are not allowed and are always removed for security purposes.
- Bug fix: When using Clinical Data Pull for CDIS, the process of fetching data from the EHR might fail with a fatal PHP error when using PHP 7.3 or 7.4. (Ticket #228374)

## Version 14.0.32

- Bug fix: When using Multi-Language Management, a text string shown in partial survey completion emails when there is no survey title was mistakenly not available for translation. (Ticket #233149)
- Bug fix: When using Multi-Language Management, the MLM setup page would fail to load in projects that have not yet set up any languages. Bug emerged in the previous release. (Ticket #233304)
- Bug fix: When using Twilio, in which one or more Twilio voice call options are enabled in the project, the voice call options would mistakenly not be displayed in any drop-downs listing all the enabled delivery preferences. Bug emerged in REDCap 13.4.0. (Ticket #233599)
- Bug fix: When viewing the "Stats & Charts" page for a report in a longitudinal project, in which a user clicks the link for the "Missing" column for a given field after having selected the Live Filter of an event that contains data for a repeating instrument (although not for the field in question), the "missing values" list of records that is returned after clicking the "Missing" link might mistakenly display extra values that are not applicable. (Ticket #232841)

## Version 14.0.31

- Medium security fix: A Reflected 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 into a specific API parameter's value that is used in several file-related and survey-related API methods. This vulnerability can be exploited only by users with a valid API token. Bug exists in all 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 into any user input that is then output on a page in REDCap (e.g., field labels, survey instructions, data displayed on a report). This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all REDCap versions.
- Bug fix: Embedding required fields into matrix groups hidden by branching logic would cause the page to crash, preventing it from being saved. (Ticket #232140)
- Bug fix: If a date, time, or datetime validated field was embedded inside the choice label of a radio or checkbox field, the width of the date/time/datetime field would mistakenly be too wide. (Ticket #232271)
- Bug fix: If alerts have been set up with an Alert Type of "SMS" or "Voice Call", the log entry on the Logging page for each alert sent would mistakenly be missing the recipients' phone numbers.
- Bug fix: If the Survey Base URL setting has been defined on the General Configuration page in the Control Center, any images that are uploaded using the rich text editor to a field label, survey instructions, etc. might not be viewable when viewing them on the survey page. (Ticket #231843)
- Bug fix: The "Administrator?" column in the "View User List by Criteria" table on the Browse Users page in the Control Center was mistakenly never updated when granular Admin Privileges were introduced to REDCap. That column currently only denotes if the user has "Access to all projects and data" privileges when it should instead display a checkmark if the user has at least one of the seven possible admin rights. (Ticket #232602)
- Bug fix: The MyCap API call "getStudyFile" was not returning any file contents for the requested file.
- Bug fix: Too many unnecessary database queries would mistakenly be executed during the Background Data Import process.
- Bug fix: When a calculated field is using a datetime field inside a datediff() function while also using "today" as a parameter (as opposed to using "now"), it might result in an incorrect calculated result on the page (although the server-side calculation process would typically correct this). (Ticket #231434)
- Bug fix: When executing a custom Data Quality rule in a longitudinal project, in which the rule's logic references a field with a blank/null value (e.g., [field]=""), the rule would mistakenly not return results from events that contain no data. (Ticket #231374)
- Bug fix: When exporting data via the Export Records API method in EAV format, in which the "fields" parameter is not provided, the API would mistakenly not return data for all project fields in the output of the API request but might instead only return the record ID field and (if the API parameter DataAccessGroups=false) the __GROUPID__  field. (Ticket #232249)
- Bug fix: When importing data for a repeating instrument, in which one of the fields on the repeating instrument is the Secondary Unique Field, in certain situations REDCap might mistakenly return an error and prevent the import process from occurring. (Ticket #229881)
- Bug fix: When importing data via the Background Data Import process in a MyCap enabled project, it might mistakenly create duplicate entries for the same record in the MyCap Participant List. (Ticket #229177)

- Bug fix: When using Multi-Language Management, "Download PDF" buttons for each language on the MLM setup page were mistakenly disabled when the project is in production mode. (Ticket #232952)
- Bug fix: When using Multi-Language Management, the survey queue page, when called directly, would mistakenly not take the language preference field into account. (Ticket #233093)
- Bug fix: When using WebDAV for file storage in REDCap, the Configuration Check page might mistakenly not display the WebDAV path on the page in one of the checks but would instead just display two double quotes where the path should be displayed.
- Bug fix: When using right-to-left languages in Multi-Language Management, the email content for translated ASIs or Alerts would mistakenly not appear in the user's/participant's email client as right-to-left. (Ticket #232158)
- Bug fix: When using the Clinical Data Mart feature for CDIS, users not having Data Mart privileges might mistakenly be able to access a Data Mart page. (Ticket #232792)
- Bug fix: When using the datetime picker on datetime fields, in which the field already has a value, clicking on the time sliders in the datetime picker would mistakenly cause the picker to close immediately. Bug emerged in the previous version. (Ticket #232350)

### Version 14.0.30

- Medium security fix: Numerous REDCap endpoints that are called via AJAX on certain pages that are oriented around project design were mistakenly not enforcing the Project Design & Setup rights requirement. This could allow someone with access to the project that does not have Design rights to access information they should not, and in the worst cases, make specific design changes to the project (e.g., copy or delete a field) when they do not have the rights to do so. Note: In order to exploit this, the user would have to have access to the project and would have to know the specific endpoints/URLs to call (and also must know some specific parameters to use). Additionally, this only affects endpoints that require Project Design & Setup rights. Bug exists in all versions of REDCap.
- Bug fix: If a user is creating a new project and selects the option to "Upload a REDCap project XML file", then chooses a file, but then selects another option (i.e., Empty project, Use a template), the Project XML file might mistakenly still be used to create the project, and in some cases might result in a fatal PHP error. (Ticket #232084)
- Bug fix: In REDCap generated PDFs that contain data for repeating instruments and/or repeating events, the repeating instance number was mistakenly not displayed in the PDF's right header above the page number. The absence of the instance number added ambiguity and made the specific instances not easily discernible from each other in the PDF.
- Bug fix: It might be possible for users/participants to bypass the @FORCE-MINMAX action tag's requirement and enter an out-of-range value for a datetime field if they tab out of the field while the datetime picker is still visible. (Ticket #231611)
- Bug fix: When attempting to delete one or more scheduled survey invitations via the right-hand checkbox in the Survey Invitation Log table by clicking the "Delete all selected" button, the invitations would fail to be deleted if the record does not exist yet (i.e., participant was added to the Participant List manually, but the participant has not yet taken the survey). (Ticket #231754)
- Bug fix: When executing Data Quality rules that return more than 10,000 discrepancies, in which one or more discrepancies have been previously "excluded" by a user, the total number of

discrepancies displayed on the page would mistakenly be listed as 10000 minus the number of exclusions (which is incorrect) rather than the total discrepancies minus the number of exclusions. (Ticket #229449)

### Version 14.0.29

- Medium security fix: A Reflected 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 into a specific API parameter's value that is used in the API File Import, File Export, and File Delete methods. This vulnerability can be exploited only by users with a valid API token. Bug exists in all REDCap versions.
- Minor security fix: An authenticated user could make a simple request to a very specific REDCap end-point, in which it would reset the REDCap Base URL and thus make the application temporarily unusable to users accessing REDCap in a web browser.
- 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 into any user input that is then output on a page in REDCap (e.g., field labels, survey instructions, data displayed on a report). This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all REDCap versions.
- Bug fix: In the previous version, it was mistakenly thought that the variable name "calculate" needed to be added to the reserved variable name list, but that turned out not to be true. Because of some new underlying code fixes, that variable name is still allowed. (Ticket #231128b)
- Bug fix: Long choice labels for fields used in Smart Charts, specifically bar charts, might mistakenly appear as too wide on the chart and thus might overlap with other text, making it hard to read.
- Bug fix: The survey queue was mistakenly not translated in MLM-enabled projects when it was displayed on the survey page itself (as opposed to when specifically viewing the survey queue page after completing the survey).
- Bug fix: When exporting an instrument PDF, the word "Confidential" would fail to be displayed in the PDF's left header by default (this excludes participant-facing PDFs, which should not display this text).
- Bug fix: When making a call to the Export Logging API method for a longitudinal project, the event name would mistakenly be omitted in the API response. (Ticket #210938)

### Version 14.0.28

- Minor security fix: The Clinical Data Pull (CDP) feature in CDIS contained a vulnerability in which a malicious user could potentially re-use a URL utilized during the "launch from EHR" process when accessing the CDP "patient portal" page, in which it might potentially allow them to access unauthorized PHI. This vulnerability is only accessible if CDP is enabled on the REDCap server.
- Major bug fix: When exporting data via the Export Records API method in EAV format with rawOrLabel="label", the value of "False" would mistakenly be returned as most of the multiple choice field values. Bug emerged in the previous release. (Ticket #230389)
- Bug fix: A missing LOINC code was added to the CDIS mapping features.

- Bug fix: In a MyCap-enabled project, some minor issues could occur via the "Create/Edit MyCap Task" and "Fix warnings" popups when the project is in production and enters draft mode.
- Bug fix: The variable name "calculate" has been added to the reserved variable name list because it could cause various unexpected issues on forms/surveys if a field has that variable name. (Ticket #231128)
- Bug fix: When a report has advanced filter logic that contains inline comments, and a user selects a Live Filter on the report page, it might cause the report page to crash with a fatal error, thus not displaying the report.
- Bug fix: When comparing two revisions/snapshots on the Project Revision History page, in which more than two columns in a given row of the comparison table display the "Preview Change" link, clicking the "Preview Change" link would only work for the left-most column that contains the link and not for any other columns. (Ticket #230991)
- Bug fix: When importing some instruments from the REDCap Shared Library that contain calc fields, line breaks existing in a calculation might mistakenly get converted to HTML "BR" tags when being imported into a project, thus causing the calculated field to throw an error when viewing it on a form/survey.
- Bug fix: When viewing the API documentation or the Documentation for Plugins, Hooks, & External Modules, the main part of the page and its content would mistakenly appear invisible if the browser window is at a specific width range. (Ticket #231012)

### Version 14.0.27

- Major bug fix: The API Delete Users method was mistakenly not checking if a user had API Import/Update privileges in the project in addition to User Rights privileges in order to successfully make a call to the API method. This bug was supposedly fixed in REDCap 13.7.28/14.0.5 LTS and 14.0.4 Standard, but mistakenly it was not. (Ticket #230626)
- Major bug fix: When the system-level setting "Allow normal users to create new projects?" is set to "No", normal (non-admin) users would mistakenly get the error "You do not have Create Project privileges!" when submitting the Create New Project page. In that situation, all users should be able to view and submit that page (unless they are not allowed to create projects via the user-level setting). Bug emerged two releases ago. (Ticket #230244)
- Bug fix: A fatal PHP error might occur for PHP 8 when loading the Form Display Logic setup dialog. (Ticket #230223)
- Bug fix: If REDCap surveys are embedded via an iframe on external web pages, in some situations the survey page might go completely blank when the page loads. (Ticket #229885)
- Bug fix: The Export Survey Link API method would mistakenly return a survey link when provided with an instrument and event in which the instrument is not designated for that particular event. In that case, the API should instead return an error. (Ticket #230491)
- Bug fix: The variable name "field_label" has been added to the reserved variable name list because it could cause some instruments to become no longer accessible in the Online Designer if a field has "field_label" as its variable name. (Ticket #230669)
- Bug fix: When MLM is active, piping would mistakenly not work on (first) survey pages when in "start over" mode.
- Bug fix: When a user simply clicks a field in the Online Designer, it would mistakenly call the "field reorder" script even though no fields were actually being reordered on the page. This

would sometimes cause the whole table to be reloaded and also could cause annoying issues such as multiple fields getting deselected when attempting to use the "Modify multiple fields" feature.

- Bug fix: When exporting data via the Export Records API method in EAV format and providing the API parameter exportDataAccessGroups=true, the DAG designations would mistakenly not get output from the API request. (Ticket #230389)
- Bug fix: When using Multi-Language Management, the mouseover tooltips for date/datetime/time validated fields would mistakenly fail to be updated with translations on MLM-enabled surveys and data entry forms. (Ticket #230546)
- Bug fix: When using an iOS device to enter data for a date/datetime/time validated field that has an accompanying datetimepicker calendar widget, the field would mistakenly lose focus with each character entered into the Text field, thus causing the user/participant to have to keep putting focus back on the field for each character needing to be entered. Bug emerged in REDCap 14.0.19 LTS and 14.3.2 Standard. (Ticket #230017)
- Bug fix: When viewing an individual email on the Email Logging page, in which the email contains a "mailto" link in the email body, the "mailto" link would mistakenly get mangled when displaying the email inside the dialog on the page. (Ticket #230319)
- Bug fix: When viewing the Record Status Dashboard or a report, if the Rapid Retrieval feature is working on the page to provide a cached version of the page, and if the RR's cache was stored when REDCap was on a previous version, in which that previous REDCap version has been removed from the web server, some images (e.g., form status icons) might not display correctly on the page and other links might lead to a 404 "does not exist" error. (Ticket #230224)

### Version 14.0.26

- Major bug fix: When the system-level setting "Allow normal users to create new projects?" is set to "No", normal (non-admin) users would mistakenly get the error "You do not have Create Project privileges!" when navigating to the Create New Project page. In that situation, all users should be able to view that page. Bug emerged in the previous release. (Ticket #230090)
- Bug fix: Certain queries on the project Logging page might mistakenly take too long to run for certain projects, thus making the page unnecessarily slow. (Ticket #229219)
- Bug fix: If using Multi-Language Management and reCAPTCHA is enabled for the public survey, the reCAPTCHA page might mistakenly throw a JavaScript error when MLM is active.
- Bug fix: When downloading an instrument PDF when the field label or section header text of a field is very long, in some cases the text in the PDF might mistakenly run over and obscure the PDF's footer text. (Ticket #205997)
- Bug fix: When exporting then importing a Project XML file, the two sub-options for the Secondary Unique Field (i.e., "Display the value..." and "Display the field label...") would mistakenly not get transferred to the new project but would resort to their default values. (Ticket #229880)
- Bug fix: When the system-level setting "Allow normal users to create new projects?" is set to "No", and a user does not have the user-level option "Allow this user to request that projects be created for them..." checked on the Browse Users page, if the user knows how to navigate to the Create New Project page (even though the links to that page have been removed in the user interface), it would mistakenly display that page and would allow them to submit a request to

create a project. Note: The project would not get created unless the admin mistakenly approved it while not realizing that this user should not be able to request new projects be created. (Ticket #229702)

- Bug fix: When users are not allowed to create or copy projects on their own, and they submit a "Copy Project" request to an administrator, in which the "Warning about miscellaneous attachments" dialog is displayed to the user on the Copy Project page, when the admin goes to approve the request, that dialog would mistakenly be displayed again (it should only be displayed initially to the user, not the admin) and thus would block the admin from successfully approving the request. (Ticket #228954)
- Bug fix: When viewing the Stats & Charts page for Report B in a longitudinal project, in which one or more events are selected for Report B, the Stats & Charts page would mistakenly not filter the data on the page to those selected events but would instead display data from all events. (Ticket #228030)