REDCap Flex Upgrade Changelog – October 2023 Upgrade (v. 13.7.14 → v. 13.7.19)

Bug Fixes and Security Fixes

Version 13.7.19

CHANGES IN THIS VERSION:

- **Major security fix:** A Stored Cross-site Scripting (XSS) vulnerability was discovered in which a malicious user could potentially exploit it by inserting custom JavaScript in a specially crafted way into specific POST parameters of an Online Designer related URL so that the custom JavaScript could be injected into the calculations of calc fields, @CALCTEXT, and @CALCDATE fields. Thus the custom JavaScript could be executed whenever anyone opens the data entry form or survey page. This could lead to privilege escalation if a malicious user tricks an administrator into viewing the instrument, thus potentially becoming an administrator themselves and able to access all projects and data. The user must be authenticated into REDCap and must have Project Design rights in order to exploit this in a project. Bug exists in all REDCap versions for the past 10 years. Note: This bug was supposedly fixed in the previous version but mistakenly was not.
- **Medium security fix:** Malicious users might be able to bypass the "Restricted file types for uploaded files" feature (if being utilized on the REDCap server) by uploading a file with an incorrect file extension into the File Repository of a project, and then changing the file's extension using the "rename file" feature. For example, an attacker could take a file named "exploit.exe", rename it to "image.jpg" on their local device, upload the file into the File Repository, rename the file to "image.exe", and then trick another user into downloading it and executing it locally. Now, REDCap prevents users from modifying the file extension of any files uploaded into the File Repository. Note: The vulnerability does not pose a risk to the REDCap server since REDCap itself never executes any uploaded files, but this only poses a risk to users who may unwittingly download and execute the file. Also, the malicious user must have File Repository privileges inside a project in order to exploit this.
- **Minor security fix:** When using Two-Factor Authentication, in which users are logging in and entering a 6-digit one-time passcode (OTP), there was no limit placed on the number of passcode submissions that can be attempted for a given user within a specific window of time. Thus, the passcode verification process was subject to brute force hacking (so long as the attempts

did not exceed the general Rate Limiter setting in REDCap). This has been changed so that the passcode verification process cannot be utilized more than 10 times per minute. If exceeded, it will now return an error.

- **Major bug fix:** When a survey participant clicks the "Save & Return Later" button on a survey, REDCap would mistakenly not always find the participant's email address (from a designated email field or from the participant list) when loading the page that displays the return code. In some cases, another participant might be sent an email containing the original participant's survey link for completing the survey. Note: Despite sending the survey link to the wrong participant, the other participant would not be able to see the original participant's responses because they do not have the Return Code. (Ticket #140765, #217097)
- Bug fix: When using Multi-Language Management, a JavaScript error might occur when piping calculated fields under specific conditions.
- Bug fix: When using Twilio or Mosio, it would mistakenly not send SMS messages to U.S. phone numbers with an 445 area code. (Ticket #216751)
- Bug fix: When using Multi-Language Management, the option to "Create from file/from scratch" would mistakenly not be available on the Control Center MLM setup page when the corresponding language creation was disabled for projects.
- Bug fix: The language variable "design_1054" mistakenly existed twice in the file "English.ini".
- Bug fix: If the settings "Allow normal users to edit their primary email address on their Profile page?" or "Allow normal users to edit their first name and last name..." are set to "Do not allow editing", a user that knows how to make a specially-crafted POST request to a specific end-point or knows how to manipulate the Profile page's user interface in a specific way would be able to modify their first/last name and/or email address, respectively.
- Bug fix: When a user imports a Project XML file that is truncated (for whatever reason) and is thus does not represent properly structured XML, in some situations REDCap might still attempt to process the XML fully without any error message, which might result in some things not getting set correctly in the resulting project, possibly unbeknownst to the user. It now attempts to do a better job of detecting if the XML is properly structured, and if not, returns an error message explaining this.
- Bug fix: When using "Azure AD OAuth2 & Table-based" authentication, users clicking the "Logout" link in REDCap would mistakenly not be successfully logged out of Azure AD. (Ticket #216423b)
- 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 531 and 726. (Ticket #216751b)

Version 13.7.18

CHANGES IN THIS VERSION:

- **Major security fix:** A Stored Cross-site Scripting (XSS) vulnerability was discovered in which a malicious user could potentially exploit it by inserting custom JavaScript in a specially crafted way into specific POST parameters of an Online Designer related URL so that the custom JavaScript could be injected into the calculations of calc fields, @CALCTEXT, and @CALCDATE fields. Thus the custom JavaScript could be executed whenever anyone opens the data entry form or survey page. This could lead to privilege escalation if a malicious user tricks an administrator into viewing the instrument, thus potentially becoming an administrator themselves and able to access all projects and data. The user must be authenticated into REDCap and must have Project Design rights in order to exploit this in a project. Bug exists in all REDCap versions for the past 10 years.
- **Medium security fix:** A user with Calendar privileges in a given project that knows how to make a specially-crafted POST request to a specific end-point might be able to edit or delete a calendar event in another project to which they do not have access.
- **Medium security fix:** A user with Data Access Group privileges in a given project that knows how to make a specially-crafted POST request to a specific end-point might be able to rename or delete a DAG in another project to which they do not have access.
- Bug fix: When using Multi-Language Management, REDCap’s auto-logout feature would mistakenly not work on the MLM setup page in some circumstances. (Ticket #216234)
- Bug fix: When printing an instrument via the option "Download this survey with saved data (via browser's Save as PDF)", a vertical line/shadow would mistakenly appear on the left side of the resulting PDF.
- Bug fix: When using Multi-Language Management, a specific warning was mistakenly not translatable via the MLM setup page.
- Bug fix: When using "OpenID Connect & Table-based" authentication, users clicking the "Logout" link in REDCap would mistakenly not be successfully logged out of OIDC. (Ticket #216423)
- Bug fix: When using Multi-Language Management, “style” HTML tags that span over multiple lines would mistakenly not work as expected when MLM is active.

Version 13.7.17

CHANGES IN THIS VERSION:

- **Major bug fix:** A user with “Alerts & Notifications” privileges in a given project that knows how to make a specially-crafted POST request to a specific end-point used for "Alerts & Notifications" functionality might be able to delete any general uploaded file that belongs to the project, whether it be an attachment uploaded via the rich text editor, a file uploaded to a File Upload field, a Descriptive Text field attachment etc. This user could potentially delete the stored edoc file for any of those such places in the project. However, it is important to note that the user can only delete files within their own project to which they have access. They cannot delete files in other projects to which they do not have access.

- **Major bug fix:** If survey invitations have been scheduled manually (i.e., not via ASI) with one or more reminders, the unsent/scheduled reminders would mistakenly not be automatically removed whenever the participant completes the survey. (Ticket #203090)
- Bug fix: The end-points used for deleting instruments and fields in a project were mistakenly using a GET request (rather than a POST request), which could make it easier for a user to get tricked into unwittingly deleting an instrument or field if a malicious user sent them a specially-crafted link to click. Such a situation would not cause any permanent damage (e.g. no data would ever be deleted), and it could be easily fixed by re-adding the instrument/field back.
- Bug fix: When using a CDIS service (CDM or CDP) to pull data from an EHR, when dealing with date values used in the FHIR requests to the EHR system, some dates might mistakenly be converted to the current timezone. This has been fixed to ensure that the date conversion only occurs in the response received from the FHIR system.
- Bug fix: When using the Protected Email Mode feature, in which an alert is set up with an attachment file and the alert is set not to send immediately but at some later time, after the alert is triggered and the email is sent, when the recipient views the email on the Protected Email Mode page, the attachment would mistakenly not be downloadable on the page but would display an error when attempting to be download it. (Ticket #212760)
- Bug fix: The hook functions "redcap_survey_page_top" and "redcap_survey_page" might mistakenly be provided with an incorrect DAG group_id value for records that have not yet been created, such as when viewing the first page of a public survey. In these cases, it would provide the DAG group_id of record "1" in the project if there exists a record named "1" when instead the group_id should be NULL. (Ticket #215884)
- Bug fix: The Unicode Transformation process might mistakenly not convert data in some database tables that have a "project_id" column in which the project_id value in the table is NULL. (Ticket #215615)
- Bug fix: Several PHP 8 compatibility issues when using certain MyCap pages/processes.
- Bug fix: The @NOW-SERVER action tag would mistakenly not set the correct value for many time-validated field types, such as a Text field with "time_hh_mm_ss" validation, whenever an instrument/survey is loaded. Instead, it might set the value as the user/participant's local time (according to their browser). (Ticket #216135)
- Bug fix: When using Multi-Language Management, for Yes/No and True/False fields, "No"/"False" was mistakenly shown instead of their associated translation in some places (e.g., Codebook). (Ticket #216265)

- Bug fix: Several different features in REDCap, in which an AJAX call returns JSON-encoded data, might get misinterpreted and thus would fail because the request failed to have the "Content-Type: application/json" header set. This would only occur for certain web server configurations. (Ticket #214401)

Version 13.7.16

CHANGES IN THIS VERSION:

- Bug fix: When renaming a record, the record name would mistakenly not get renamed on the Email Logging page. This would not cause any issues other than the Email Logging saying that an email belongs to the wrong record. (Ticket #215100)
- Bug fix: The Unicode Transformation process might mistakenly not display correct information regarding whether or not some specific steps in the process need to be completed.
- Bug fix: The "field suggest" feature when using the Logic Editor was mistakenly no longer appearing as of REDCap 13.7.13 LTS and 13.9.3 Standard Release. (Ticket #215285)
- Bug fix: When using the Clinical Data Mart design checker's "fixDesign" process, a fatal PHP error might occur in certain situations.
- Bug fix: Some project pages might fail with a fatal PHP error when using PHP 8 due to the calling of an undefined PHP constant in the External Module Framework. (Ticket #215348)
- Bug fix: When using Multi-Language Management, the "Access Denied!" a message that appears on data entry forms when a user has no access was mistakenly not a translatable element in MLM. (Ticket #215504)
- Bug fix: In a MyCap-enabled project, slider labels (displayed above or next to the slider) were not displaying correctly in the MyCap config JSON and thus might cause issues in the MyCap mobile app.
- Bug fix: When using the Data Resolution Workflow along with Data Access Groups in a project, if a user attempts to assign a data query to a user, in some situations the drop-down list of assignable users would mistakenly list users that are not currently eligible to be assigned to the data query because they are not currently assigned to the record's DAG. It should only list users that are currently in the record's DAG (or users not in any DAG) if the record itself is assigned to a DAG. (Ticket #213770)
- Bug fix: When using CDIS, the SMART on FHIR authentication process was causing incorrect scope levels to be applied, specifically impacting Cerner users. The issue prevented the proper assignment of the "user" level during authentication, thus potentially leading to authorization errors.
- Bug fix: The auto-fill form/survey feature for administrators might mistakenly fail for most/all time validated fields. (Ticket #215684)
- Bug fix: When an [X-event-name] Smart Variable is prepended to a field variable (especially in combination with an [X-instance] Smart Variable) in

logic, calculations, or piping, it might cause the evaluation of the logic/calc/piping not to be performed successfully. For example, for [previous-event-name][field], the direct previous event might be used when instead the previous designated event for that field's instrument should be used. (Ticket #214317, #213503)
- Bug fix: If using an HTML "style" tag inside user-defined text (e.g., field label, survey instructions), the CSS styles inside the tags might mistakenly not work on the page if line breaks or carriage returns occur anywhere inside the opening and closing style tag. (Ticket #215693)

Version 13.7.15

CHANGES IN THIS VERSION:

- **Major bug fix:** When using randomization while in production status, if a user is uploading a new allocation table to be appended to the existing production allocation table, in which the development allocation table happens to exactly match all the production allocations after the allocation upload has occurred, all the production allocations would mistakenly be erased, which would also remove the "randomized" status for any already randomized records. This is extremely rare, but is extremely destructive and difficult to restore back to its previous state.
- Bug fix: When viewing the MyCap participant list, the Baseline Date might mistakenly be displayed in an incorrect date format.
- Bug fix: A user that does not have Project Setup privileges in a project could potentially exploit a missing user rights check on the endpoints where field attributes are modified in the Online Designer by crafting special HTTP requests to those specific endpoints. This does not allow the user to do anything other than add new fields or edit the attributes of existing fields.
- Bug fix: When viewing the Record Status Dashboard in certain cases when using PHP 8, the page might crash with a fatal PHP error. (Ticket #214370)
- Bug fix: When users make API requests, the full API token was mistakenly being logged in the redcap_log_view table for each request. This is not typically an issue because such values in that table are not exportable via the front-end user interface but are only accessible via direct database access. However, if some institutions are sending the full export of their redcap_log_view table to their local security office, the logging of the API token in that table could be problematic. The API token will now be redacted in the redcap_log_view table. (Ticket #214322)
- Bug fix: When users delete or regenerate their API token in a project, the value of the old token was mistakenly not being logged on the project's Logging page.
- Bug fix: Fixed issue with the CDIS "Break the Glass" feature. When attempting to restore a serialized list of patients, an error is thrown due to the DateTime class not being listed within the "allowed_classes" parameter of the unserialize function. (Ticket #214670)

- Bug fix: An administrator with only “Install, upgrade, and configure External Modules” admin privileges might not be able to view certain External Module pages or perform certain External Module operations, such as accessing the EM Manage page in the Control Center. (Ticket #214721, #214722)
- Bug fix: An issue might occur when downloading a file from a File Upload field when REDCap is hosted on Google Cloud Platform due to the usage of an unnecessary project_id prefix for Google bucket file storage.
- Bug fix: The notification for the Unicode Transformation process on the Configuration Check page might mistakenly not be displayed on the page anymore after step 2a of the process has been completed. It should not go away until all 4 of the steps are completed.
- Bug fix: When attempting to access the "App Data Dumps" on the REDCap Mobile App page in a project, if any of the data dump files somehow can't be found in the file system (which would be unexpected), the page would crash with a fatal PHP error. From now on, it will merely skip any files in this situation. (Ticket #215007)
- Bug fix: When date or datetime fields are piped into the choice label of a drop-down field, in which the date/datetime field has MDY or DMY date format and also exists on the same page as the drop-down field, the date/datetime values might not get piped in the correct format but may appear in the drop-down as a mangled date/datetime value.