

**February 2025 Security and Bug Fixes**

**Major Security Fixes**

* 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), specifically targeting the "href" attribute of a hyperlink. This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all REDCap versions.
* An SQL Injection vulnerability was found on the User Rights 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 when adding new User Roles. This can only be exploited by authenticated users. Bug exists in REDCap 10.3.3 and higher.
* 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), specifically targeting the "href" attribute of a hyperlink. This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all REDCap versions.
* An SQL Injection vulnerability was found on the User Rights 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 when adding new User Roles. This can only be exploited by authenticated users. Bug exists in REDCap 10.3.3 and higher.

**Minor Security Fix**

* An Insecure Direct Object References (IDOR) vulnerability was found, in which a malicious user could potentially exploit it by manipulating the URL of the Sponsor Dashboard page in a specially crafted manner. This could allow the attacker to view a sponsor's Sponsor Dashboard page (and view the names and emails of all their sponsees that they sponsor) and could allow the attacker to request actions on behalf of the sponsor, such as requesting that a sponsee's password be reset, that the sponsee be suspended, etc. Administrators should be allowed to view a sponsor's Sponsor Dashboard, but regular users should only be able to view their own Sponsor Dashboard. Note: This vulnerability is only exploitable if the User Sponsor functionality is being utilized in REDCap

**Bug Fixes**

* If a MyCap-enabled PROMIS instrument is part of a Health Measure battery, the instrument was not functioning in a series as repeating for selected events.
* The "Require reversal" setting for the "Spatial Memory" active task for MyCap should not have been displayed on the MyCap task settings page for that specific active task because it was never utilized on the MyCap mobile app side.
* When MLM is active on a form/survey that contains Smart Charts in translatable labels, the Smart Charts would get lost during rendering of the field translations.
* When downloading a PDF of a survey instrument or when REDCap is storing a PDF Snapshot of a survey instrument, certain HTML tags (most notably BR tags) that exist in the survey instruction text might mistakenly get stripped out before being properly processed into line breaks, etc. for the PDF. Bug emerged in REDCap 14.5.0.
* When exporting an individual instrument's translations on the MLM setup page, the settings from the MLM export dialog were not properly observed.
* When translating text via MLM for section headers and matrix headers, "line breaks" were not properly preserved when MLM is active on a form/survey.
* A race condition exists during the record randomization process in which two records being randomized simultaneously on a data entry form could cause a fatal PHP error to occur or possibly cause other issues if both records currently do not exist yet when the randomization process is performed.
* If a project has only one form and the current record does not exist yet, the project will normally try to bypass the Record Home page and redirect the user directly to the data entry form as a convenience. If Form Display Logic is being utilized and the logic always evaluates to false for new records in this case before they are created, this will cause an infinite redirect loop on the page and prevent users from creating new records using the user interface.
* If a proxy server is utilized for REDCap and is configured on the General Configuration page in the Control Center, the AI features in REDCap would mistakenly not work. Bug emerged in REDCap 15.0.0.
* In certain situations, some REDCap cron jobs might mistakenly not get executed for a very long time compared to when they are expected to run if some other prioritized jobs consistently get run by the REDCap cron for a disproportionate amount of time. The prioritization logic that determines which jobs are run and when they are run has been modified slightly so that REDCap will occasionally prioritize cron jobs that have not been run in a long time to ensure that all jobs get a chance to run closer to their expected interval.
* In specific unknown circumstances, REDCap might mistakenly crash due to a "Detection\MobileDetect" PHP class not being found.
* In very specific cases in multi-arm projects where one arm contains only one event while then other arms do not contain any events, the "Download arms (CSV)" option on the "Define My Events" page would display a confusing error message when clicked, thus preventing the user from downloading the CSV file.
* When a survey has the setting "Show or hide the Submit buttons" set to "Always hide", if any field values change while viewing the survey page, and then the survey page is closed (browser is closed or tab is closed), the "Leave site?" prompt would be displayed. The prompt should not be displayed in that situation since there is no way to submit the survey page.
* When creating new arms in a project via CSV upload on the "Define My Events" page or via the API, it would mistakenly allow users to add arms with an arm number higher than 99, which is supposed to be the maximum possible value. Note: If users have done this previously, there should not be any negative consequences in the project.
* When importing data using the Data Import Tool, in which out-of-range values are being imported for text fields with min/max validation ranges, the orange warning would mistakenly not be displayed on the page for those fields.
* When the Secondary Unique Field is enabled in a project and multiple users or survey participants are submitting the same value for the SUF at nearly the same time, the SUF uniqueness check would fail to catch duplicates because of a lack of server-side checking when a form/survey is submitted. To prevent duplicate values in the future for the SUF in this situation, REDCap now employs post-submission server-side checking, in which it will not save the duplicate value for whoever submits their page last, and additionally, it will display a warning popup letting them know why their value could not be saved and for them to enter a different value for the field.
* When using Multi-Language Management in a project where alerts are translated via MLM, if the alert is set to send immediately (rather than with a delay), the alert might be sent not with the translated text but instead with the original default language text.
* When using the Background Data Import process, in which the records being imported contain hundreds or thousands of repeating instances within each record, database performance could be impacted due to inefficient query methods during the process of uploading the data file.
* A fatal PHP error might occur when using REDCap Messenger in specific situations.
* A few references to the old domain "redcap.vanderbilt.edu" still existed in some "User Guides and Wizards" listed on the "Help & FAQ" page. Those have been updated to have the "redcap.vumc.org" domain name.
* If survey invitations are scheduled (manually or via ASI) and then the survey instrument is completely deleted from the project, any scheduled (but unsent) invitations or reminders would mistakenly still get sent to the participant.
* If using the Mandrill third-party email service for outgoing emails, in some situations (e.g., the Mandrill account runs out of tokens), emails would get "queued" in Mandrill and never get sent, but REDCap would count these emails as having been successfully sent. In this case, REDCap will appropriately note the emails as not successfully sent.
* In certain situations when performing a fresh installation of REDCap, the install page might fail with a fatal PHP error.
* In rare situations when viewing the record status dashboard in a project, the page might crash due to a PHP error, especially if the Rapid Retrieval feature is enabled for the system.
* When a project contains Data Access Groups and a user modifies the "Page X of Y" drop-down list on the Record Status Dashboard after "[No Assignment]" has been selected in the DAG drop-down list, the page would reload but mistakenly have the "All" DAG option auto-selected.
* When a user account is deleted from the system via the Browse Users page in the Control Center, in which the user being deleted is a sponsor for one or more users, the deleted user would fail to be removed as a sponsor for the other users.
* When a user attempts to send an announcement or message to a MyCap participant via the MyCap Participant List page, in which the announcement/message fails to send for whatever reason, the user would mistakenly not be notified about the failure, and the announcement/message would be logged in REDCap as if it had sent successfully.
* When an instrument PDF is generated/downloaded or is stored as a PDF Snapshot, if all the fields that follow a section header on the instrument are hidden by branching logic or action tags, in which those fields are the last fields on the instrument but are not the last fields of the whole PDF, the section header would mistakenly be displayed in the PDF when it should instead be hidden/not visible. (Ticket #249551)
* When executing Data Quality rules in multi-arm projects in which fields used in the rule's logic are utilized on some arms but not others, while at the same time one or more of the logic fields are used on repeating events, this could cause the DQ rule to return false discrepancies for records that don't exist in some arms.
* When performing a data import for repeating instruments or repeating events, in which the "redcap\_repeat\_instance" value being imported begins with the text "new" but is not the exact word "new" (e.g., new-instance), the data would get imported but might mistakenly get orphaned in a way that it is not accessible for editing/deleting in the user interface afterward. The import process will now only allow a positive integer or the exact word "new" to be used as a valid value for "redcap\_repeat\_instance".
* When the Double Data Entry feature is enabled in a project and a user is merging two records into a new third record on the Data Comparison Tool page, if a Text or Notes field is selected on that page, in which the selected field's value contains an apostrophe, it would cause a JavaScript error that would mistakenly prevent that value from being included as part of the merge process (unbeknownst to the user) when creating the new record.
* When user account expiration emails are being sent out by the system, the outgoing email might mistakenly have the incorrect person/sponsor CC'd in the email in certain circumstances.
* When using Multi-Language Management on an instrument where fields are embedded, fields embedded in a field that is excluded from MLM translation would mistakenly be invisible on the page.
* When using the Data Resolution Workflow and a custom Data Quality rule has real-time execution enabled, if the DQ rule is violated by a user via data entry on a form and then the user "verifies" the field's value, the Data Quality rule would mistakenly still show a violation as existing if the form is saved again. This only occurs if the form is a repeating instrument or is on a repeating event.
* When using the Data Resolution Workflow and a custom Data Quality rule has real-time execution enabled, if the rule is violated by a user via data entry on a form and the user opens/closes/responds to a data query or verifies/de-verifies the field's value, the button in the "Data Quality rules were violated" dialog for that DQ rule would mistakenly not get updated with the new number of comments and new icon representing the current state of the data query.