REDCap Version	Description
14.5.41	Critical bug fix: When a project is in draft mode and an administrator approves their drafted changes, or if the user clicks Submit Changes for Review in the Online Designer where the changes are approved automatically, the process would mistakenly fail with a fatal PHP error. Bug emerged in the previous release. (Ticket #248136)
14.5.40	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 the attributes of fields (e.g., field label) when viewing and saving fields on the Online Designer's field-view page. If successfully exploited, this could allow the attacker to remotely execute arbitrary code on the REDCap server. Note: Only authenticated users are able to exploit this. This issue was supposedly fixed in REDCap 14.5.38 LTS and 15.0.4 Standard Release, but it was only partially fixed. This vulnerability exists in all versions of REDCap.
14.5.40	Bug fix: Some text on the Calendar page in a project, specifically the Agenda tab, might mistakenly not be displaying as translated but would be in English if the project is set to use a different language. (Ticket #247305b)
14.5.40	Bug fix: When using Multi-Language Management together with MyCap in a project that is in production status, the MyCap project config JSON that is consumed by the MyCap mobile app was mistakenly not getting updated when MLM changes were made on the MLM setup page.
14.5.39	Critical bug fix: Any survey pages or data entry forms that contain calculated fields would mistakenly crash and never load due to a fatal PHP error.
14.5.38	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 any REDCap logic that is stored in a project (e.g., calculations, branching logic, data quality rule logic, report filter logic). Note: Only authenticated users are able to exploit this. This vulnerability exists in all versions of REDCap.
14.5.38	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 the attributes of fields (e.g., field label) when viewing and saving fields on the Online Designer's field-view page. If successfully exploited, this could allow the attacker to remotely execute arbitrary code on the REDCap server. Note: Only authenticated users are able to exploit this. This vulnerability exists in all versions of REDCap.
14.5.37	Bug fix: In a MyCap-enabled project, a user clicking the "Messages" link for a participant on the MyCap Participant List page might mistakenly receive a "Missing/Invalid Participant" message. (Ticket #246982)
14.5.37	Bug fix: In the Online Designer when editing a field that has field validation, in which the field has both min and max validation values, if the user changes the validation type and then puts their cursor into the min validation text box, they may get stuck in a never-ending validation error loop. (Ticket #247376)
14.5.37	Bug fix: REDCap mistakenly did not allow dropping of text (e.g., from Word) into input elements in the Online Designer.
14.5.37	Bug fix: The "deceased date/time" value of a patient whose data is pulled via CDIS might mistakenly contain a leading space, thus leading to field validation issues in CDIS projects when the data is being imported from the EHR. (Ticket #247705)
14.5.37	Bug fix: The special function isnumber() would mistakenly return True when provided with a number with a leading zero (e.g., "02"). It now returns False for any text strings that are numbers with leading zeros.

14.5.37	Bug fix: When a custom Record Status Dashboard is ordered by a project's record ID field in "Descending order", the dashboard will mistakenly not display the records in the correct order if the first instrument in the project is a repeating instrument or if it exists on a repeating event. (Ticket #247891)
14.5.37	Bug fix: When using "Copy" option for the instrument-level "Choose action" button in the Online Designer, the instrument would fail to be copied and return a vague error message if a Text field on the instrument contains field validation that does not exist as a valid field validation type on the REDCap server.
14.5.37	Bug fix: When using any "X & Table-based" authentication method together with Two-Factor Authentication enabled in REDCap, in which the "Enforce two-factor authentication ONLY for Table-based users" setting is set to "Yes" and the "Enable the Google/Microsoft Authenticator app option for 2FA" setting is enabled, the QR code and setup procedure information for setting up the Authenticator app would mistakenly be displayed to non-Table-based users, such as on the user's Profile page and immediately after verifying their primary email address. (Ticket #247942)
14.5.37	Bug fix: When using the "Custom Surveys for Project Status Transitions" feature together with the Survey Base URL feature, the custom survey that is loaded in an iframe on the page for a Project Status Transition would load but might mistakenly fail to be submitted due to a cross-origin JavaScript security permission error. (Ticket #240644b)
14.5.37	Bug fix: When viewing a survey that contains hyperlinks in the survey instructions, survey completion text, or in field labels that utilize the rich text editor, the hyperlink's text might mistakenly be locked at a specific font size and thus would look strange adjacent to other text. (Ticket #246917b)
14.5.36	Major bug fix: The upgrade process might fail to complete when executing the upgrade SQL script to upgrade to the previous version. (Ticket #247576)
14.5.35	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.
14.5.35	Major security fix: An Insecure Direct Object References (IDOR) vulnerability was found, in which a malicious user could potentially exploit it by manipulating an HTTP request in a specially crafted manner when uploading files for File Upload fields on survey pages and data entry forms. This could allow the attacker to download any file that has been uploaded into the project, potentially containing sensitive/private information. The files that could be downloaded include those uploaded to File Upload fields, to the File Repository, or any other files that have been generally uploaded into the project in the past. Note: This vulnerability does not allow someone to download files from another project, but only files within the current project, such as files associated with a different record or a different field, event, or instance within the same record.
14.5.35	Bug fix: A missing LOINC code was added to the CDIS mapping features.
14.5.35	Bug fix: If a multiple choice field has one or more non-integer numeric codings (e.g., 0.5), in which the field is used in a calc or CALCTEXT field that utilizes mathematical addition (e.g., [field1]+[field2]), the resulting calculation might not always be mathematically correct in certain situations, such as if some fields used in the calculation have a blank/null value. (Ticket #246718)
14.5.35	Bug fix: In certain MLM setup situations, the Survey Queue might fail to translate completely.
14.5.35	Bug fix: In certain situations, the Submit buttons at the bottom of survey pages might mistakenly not be wide enough. Bug emerged in the previous release.

14.5.35	Bug fix: Some text on the Scheduling and Calendar pages in a project might mistakenly not be displayed as translated but would be in English if the project is set to use a different language. (Ticket #247305)
14.5.35	Bug fix: When performing a Data Search on the "Add/Edit Records" page, in which the search results include a match on a record's record ID/name while the first instrument in the project is not designated for certain events in a longitudinal project, the search results might mistakenly return a result pointing to an event where the first instrument is not designated, and thus the user clicking the search result would lead to an "Access Denied" error. It will now not output such search results in this specific case. (Ticket #247507, #247508)
14.5.35	Bug fix: When performing a Data Search on the "Add/Edit Records" page, in which the search results include a match on a record's record ID/name while the user does not have view access to the first instrument in the project (where the record ID field is located), clicking the search result would mistakenly take the user to a form to which they do not have access, which would display an error message and could be confusing. It will now take the user to the Record Home Page for that record in this specific situation. (Ticket #247510)
14.5.35	Bug fix: When renaming an instrument that is enabled as a survey via the "Choose action" button in the Online Designer, if the user enters a new instrument name that contains an apostrophe, then when REDCap asks if the user wants to also change the survey title to that value, the "Yes" button in the dialog would mistakenly do nothing due to a JavaScript error. (Ticket #247526)
14.5.35	Bug fix: When using "Large" or "Very large" as the survey text size for a survey that has horizontally-aligned checkboxes, the first checkbox of a field would appear to be slightly cut off on the left side. (Ticket #247466)
14.5.35	Bug fix: When using OpenID Connect for authentication, the pre-filling of a user's first/last name and email address in their Profile might mistakenly not occur for certain OIDC setups. (Ticket #246812)