SimpleRisk Release Notes November 2019 - Version 20191130-001

SimpleRisk version 20191130-001 includes bug fixes, security updates, the introduction of a new integration extra for Jira. It also includes the introduction of a new update method enabling users to click once to upgrade both the application and the database. If you are not already running SimpleRisk, then follow the standard installation instructions. If you are currently running the 20190930-001 release of SimpleRisk, then you will need to extract the new files over the old ones (back up your config.php first) and then run the /admin/upgrade.php script to upgrade your database.

The complete list of changes for this release is below:

- **New Features**
    - Added a selection to view the Date Closed value on the Dynamic Risk Report.
    - Updated existing multi-select dropdowns to be searchable and scrollable.
    - Added the ability to search tags when filtering by tags in the Dynamic Risk Report.
    - Added a new filter on the Compliance Active Audits page that allows you to filter based on the "Test Name" column.
    - Added a new filter on the Compliance Past Audits page that allows you to filter based on the "Test Name" column.
    - Added a new "Actions" column in the Audit Timeline report enabling the user to initiate a new audit of the test, view active audits of the test, or view past audits of the test directly from the page.
    - Updated the Team field for assets to be a multi-select dropdown.
    - Updated the "Associated Frameworks" under the Audit Timeline report so that only active frameworks are displayed.
    - Added the ability for a user to select any document type as a parent in the Document Hierarchy on the Governance page.
    - Removed the ability to create a risk subject with only whitespace characters.
    - Removed the "report requires PHP >= 5.5" message if you are running PHP >= 5.5.
    - Added a health check to detect an outdated version of PHP.

- **Security**
    - Added additional code to prevent a time-based account enumeration attack on login.
    - Fixed a CSRF vulnerability with the new one-click-upgrade functionality.
    - Fixed a SQL Injection vulnerability with audit trail logs.
    - Fixed a Stored XSS vulnerability with the new risk appetite functionality.
    - Fixed a Stored XSS vulnerability with the Frameworks and Controls tabs.
    - Fixed an issue where any user could access the list of Framework Controls.
    - Fixed an issue where an unprivileged user could change the risk levels.

- **Usability**
  - Added the "Date Closed" column in the Dynamic Risk Report.
  - You can now sort by residual risk within different groups of risks in the Dynamic Risk Report.
  - Added a filter for “Test Name” on the past audits page.
  - Updated Assets team select to a multi-select dropdown.
  - Updated the “Associated Frameworks” under the Audit Timeline so that only active frameworks are now displayed.
  - Updated the Audit Timeline report and added a new “Actions” column allowing users to re-open tests directly from the report.

- **Bug Fixes**
  - The missing "Initiate Test" functionality was added back to the Initiate Audits page.
  - Fixed an issue where the pop up menus were no longer able to be scrolled through.
  - Fixed an issue where filtering by an asset or asset group in the Dynamic Risk Report did not work.
  - Fixed an issue where you could not make a tag that contained spaces in it.
  - Fixed an issue where you could not sort by Residual Risk Score in the Dynamic Risk Report after grouping by risk level.
  - Fixed an issue where the Dynamic Risk Report did not properly group by risk level when using custom risk level names.
  - Fixed an issue where changing tabs in the Configure -> Settings menu caused the Risk Appetite slider to disappear until the page is refreshed.
  - Fixed an issue where the "All" button on the Risk Appetite Report did not expand to show all risks under the selected tab.
  - Fixed a spelling issue for "Mitigation Supporting Documenttation" under the Mitigation tab in the Configure, Extras, and Customization menus.
  -

- **Notes**
  - Beginning with the 20170102-001 release, SimpleRisk utilizes a new API for the Management section as well as several of the reports. In order for it to work properly, you will need to enable the API by setting “AllowOverride all” in your Apache configuration file. This tells Apache to utilize the newly included .htaccess file in the /api directory.
  - As of the 20151219-001 release, we will no longer provide the SQL files for the various languages. Instead, users should use the Installer Script to perform their SimpleRisk MySQL database installation. If you would like to inspect the MySQL

database schema before installing, the files can still be found under the “db” directory included with the Installer Script.

- In performing some testing with a newer version of PHP, it appears that PHP has removed the standard JSON extension as of PHP 5.5rc2 due to a license conflict. This functionality is used in SimpleRisk’s graphing library. If you notice that your pie charts are not displaying properly, you may need to install the “php5-json” package for these charts to work as expected.
- A SimpleRisk user noted that they were having difficulty logging in with the default username of “admin” with password of “admin”. Upon investigation, it was discovered that PHP was enforcing secure cookies, but the application was not using SSL, so the session values were not set. This may be an isolated instance, but if you experience this issue, try installing a SSL certificate and run SimpleRisk over HTTPS to fix it.