SimpleRisk Release Notes November 2019 - Version 20200328-001

SimpleRisk version 20200328-001 includes bug fixes, security updates, and the new overhauled Dynamic Risk Report. It also includes several quality of life updates as well as new health check features. If you are not already running SimpleRisk, then follow the standard installation instructions. If you are currently running the 20191130-001 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 column filters at the top of the Dynamic Risk Report. These filters are also saved in any new saved selection reports that are made.

- **Security**
    - Added the ability to set SimpleRisk to make requests via a proxy through the SimpleRisk UI. This setting is found under "Configure" → "Settings" → "Security".
    - Fixed multiple XSS vulnerabilities.
    - Fixed multiple SQL injection vulnerabilities.
    - Open sessions are now immediately invalidated when a password is reset.
    - When account lock-out occurs any active sessions for that account are also invalidated.

- **Usability**
    - Added a new audit log type for User events.
    - Now when a user assigns an asset to a risk if they then report on a group of assets that contain that asset, it is now displayed when the group hasn't also been added to the risk.
    - Risks and Assets report has been updated to show risk's locations/teams in the rows instead of the asset's row
    - Group names are now included on the Assets by Risk report in brackets.
    - The Dynamic Risk report has had a UI overhaul. This results in less screen clutter with all the same features and more.
    - The Audit trail is updated when a framework is deleted.
    - After adding a test to a control you are now brought back to the same place you were when you clicked "Add Test".
    - Changing user permissions while a session is open will now immediately take effect without the need to logout.

- Added the ability to control whether the "High Risk Report" is based on inherent or residual risk score.
- Added a health check to see if an Extra is compatible with the SimpleRisk instance version.
- Added a health check to see if an instance is running the most recent version of an Extra.
- Sorted the "Mitigation Controls" dropdown when planning a mitigation in alphabetical order.

● **Bug Fixes**
- Fixed a bug where using the "Group by" feature on the Dynamic Risk Report would show both a column header and footer when that was not necessary.
- Updated a function that caused an error when the SimpleRisk Base URL was not set.
- Fixed a small bug when updating your user profile language while selecting "--".
- Fixed a bug where users would not receive password reset e-mails without setting the simplerisk_base_url.
- Fixed an issue where STRICT_TRANS_TABLES would throw an error if too many characters were entered in the Compliance related fields.
- Fixed a but where the risk levels for "Custom" Classic risk score were not being set properly.
- Removed Control Regulation from Add and Remove Values as this is now governed by the Governance section of SimpleRisk.
- Fixed a UI bug that would occur when a Frameworks name was too long.
- Fixed an issue where reporting with Risks and Assets would cause an incorrect maximum quantitative loss when an asset group was attached to a risk.
- Fixed a bug that was causing Site/Location and Asset Valuation for assets to not accept new changes.
- Fixed various issues that occur when SimpleRisk is run from a sub-directory of the virtualhost.
- Fixed a bug where all pages were making an unnecessary call to the SimpleRisk update server.
- Fixed a bug where circular references could be made for frameworks using parent/child associations.
- Fixed undefined index errors on the Risk and Controls report.
- Fixed a bug where the Contributing Risk popup window was named "SimpleRisk OWASP Calculator" instead of "SimpleRisk Contributing Risk Calculator"
- Added a check for proper mysql database user permissions to the health check.

● **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.