

SimpleRisk Release Notes

Version 20130916-001

This version addresses a significant security issue that was reported to me on 9/16/2013 by Ryan Dewhurst which affects all previous versions of SimpleRisk. In order to allow my users enough time to update, I am not disclosing the nature of the vulnerability, but it will eventually be disclosed via Ryan's public CVE. All SimpleRisk users are strongly encouraged to update to this new version of the software as soon as possible. If you are not already running SimpleRisk, then follow the standard installation instructions. If you are currently running the 20130915-001 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 new features for this release are below:

- Security Enhancements
 - Fixed several potential Cross Site Scripting issues.
 - Fixed several potential HTTP Response Splitting issues.
 - Added a HTTPOnly flag to the session cookie.
 - Added a SECURE flag to the session cookie if the connection is initiated via HTTPS.
 - Added Content Security Policy (CSP) headers to provide additional protection against certain types of attacks.
 - Added the X-XSS-Protection header to ensure that browser Cross Site Scripting filtering is enabled.
- Bug Fixes
 - Fixed an issue with CVSS scoring that affects the case where the calculated Impact subscore is zero.