SimpleRisk Bill of Materials (BOM)

(Last Updated 2023-03-28)

SimpleRisk Core: This is the free and open source offering from SimpleRisk that also forms the basis for both our on-prem and hosted offerings. It is licensed under the Mozilla Public License (MPL) 2.0.

SimpleRisk Core Dependencies

Component is automatically updated via PHP Composer

Component is monitored but must be manually managed

Component is obsolete and needs to be replaced

Software Name/Version	Description	Location	License Information
Apache's APR1 MD5 Hashing Algorithm in PHP	Apache's APR1-MD5 algorithm in pure PHP	/vendor/whitehat101/apr1-md5	MIT license
Bootstrap	The most popular HTML, CSS, and JavaScript framework for developing responsive, mobile first projects on the web.	/vendor/twbs/bootstrap	MIT license
Bootstrap Multiselect		/js/bootstrap-multiselect.js	Apache License, Version 2.0
CA-Bundle (1.3.5)	Small utility library that lets you find a path to the system CA bundle, and includes a fallback to the Mozilla CA bundle.	/vendor/composer/ca-bundle	MIT license
Color picker (Unknown)	A simple component to select color in the same way you select color in Adobe Photoshop.	/js/colorpicker.js	MIT license and GPL
Composer	Dependency Manager for PHP	/vendor/composer/composer	MIT license
Composer Installers Extender	A plugin for Composer that allows	/vendor/oomphinc/composer-installers-extender	MIT license

	any package to be installed to a directory other than the default `vendor` directory within a project on a package-by-package basis.		
CSRF-Magic (1.0.5)	Automatic CSRF protection for PHP applications	/vendor/simplerisk/csrf-magic	BSD-2-Clause license
Datatables (1.10.12)	Add advanced interaction controls to your HTML tables	/js/dataTables.rowGroup.min.js /js/dataTables.rowReorder.min.js /js/jquery.dataTables.js	MIT license
Date Range Picker (2.1.25)	Pop up calendars for selecting dates, times, or predefined ranges like "Last 30 Days".	/js/daterangepicker.js	MIT license
Doctrine Lexer (1.2.3)	PHP Doctrine Lexer parser library that can be used in Top-Down, Recursive Descent Parsers. Note: Required by phpmailer	/vendor/doctrine/lexer	MIT license
Duo PHP	Note: The use of this package has been deprecated and the SimpleRisk Core now supports TOTP authentication through the pragmarx/google2fa package.	/vendor/duosecurity/duo_php	View license
EasyUI for jQuery (1.5.3)	EasyUI framework helps you build your web pages easily.	/js/datagrid-filter.js /js/jquery.draggable.js /js/jquery.droppable.js /js/jquery.easyui.min.js	freeware
Epiphany (1.0.1)	A micro PHP framework that's fast, easy, clean and RESTful.	/vendor/raid-software/epiphany	View license
Email Validator (3.2.1)	A library for validating emails against several RFCs Note: Required by swiftmailer	/vendor/egulias/email-validator	MIT license

FontAwesome (5.15.4)	Font Awesome, the iconic SVG, font, and CSS framework.	/vendor/components/font-awesome	• The Font Awesome font is licensed under the SIL Open Font License - http://scripts.sil.org/OFL • Font Awesome CSS, LESS, and SASS files are licensed under the MIT License - http://opensource.org/licenses/mit-license.html • The Font Awesome pictograms are licensed under the CC BY 3.0 License - http://creativecommons.org/licenses/by/3.0/
GetText (4.8.7)	PHP gettext manager Note: Required by simplesamlphp	/vendor/gettext/gettext	MIT license
GetText Languages (2.9.0)	gettext languages with plural rules Note: Required by simplesamlphp	/vendor/gettext/languages	MIT license
Google2FA (8.0.1)	Google2FA is a PHP implementation of the Google Two-Factor Authentication Module, supporting the HMAC-Based One-time	/vendor/pragmarx/google2fa	MIT license

	Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC 6238.		
HighCharts (10.3.1)	Highcharts JS is a JavaScript charting library based on SVG, with fallbacks to VML and canvas for old browsers.	/vendor/node_modules/highcharts	SimpleRisk has purchased a perpetual Highcharts OEM License for unlimited installations. This license applies for all customers using SimpleRisk, regardless of whether they are utilizing it in a hosted or on-premise installation.
HTMLPurifier (v4.14.0)	Standards compliant HTML filter written in PHP	/vendor/ezyang/htmlpurifier	LGPL-2.1 license
Jobby (v3.5.0)	Manage all your cron jobs without modifying crontab.	/vendor/hellogerard/jobby	MIT license
jQuery		/vendor/components/jquery	MIT license
jQuery BlockUI (v20141123)	Simulate synchronous behavior when using AJAX, without locking the browser.	/js/jquery.blockUI.min.js	MIT license and GPL
jQuery DateTimePicker	Unobtrusively add a datetimepicker, datepicker or timepicker dropdown to your forms.	/js/jquery.datetimepicker.full.min.js	MIT license
jQuery UI	A curated set of user interface interactions, effects, widgets, and themes built on top of the jQuery JavaScript Library.	/vendor/components/jqueryui	MIT license
JSON Schema	A PHP Implementation for validating JSON Structures against a given Schema with	/vendor/justinrainbow/json-schema	MIT License

	support for Schemas of Draft-3 or Draft-4.		
Laminas Escaper (2.6.1)	Securely and safely escape HTML, HTML attributes, JavaScript, CSS, and URLs	/vendor/laminas/laminas-escaper	BSD-3-Clause license
Laminas ZendFramework Bridge (1.1.1)	Alias legacy ZF class names to Laminas Project equivalents. Note: Required by Laminas Escaper. Reliance on PHP >= 7.2 prevents upgrading beyond 1.1.1. Current version is 1.6.1.	/vendor/laminas/laminas-zendframework-bridge	BSD-3-Clause license
Moment.js	A JavaScript date library for parsing, validating, manipulating, and formatting dates.	/vendor/moment/moment	MIT license
Opis Closure	A library that can be used to serialize closures (anonymous functions) and arbitrary objects. Note: Required by Jobby	/vendor/opis/closure	MIT license
PHP Cron Expression Parser (v3.3.2)	CRON for PHP: Calculate the next or previous run date and determine if a CRON expression is due Note: Required by Jobby	/vendor/dragonmantank/cron-expression	MIT license
PHP Enum (1.7.7)	PHP Enum implementation inspired from SplEnum Note: Required by zipstream-php. Reliance on PHP >= 7.2 prevents upgrading beyond 1.7.7. Current version is 1.8.4.	/vendor/myclabs/php-enum	MIT license
PHP Standards Recommendations	Allow developers to create cache-aware libraries that can be integrated into existing	/vendor/psr	MIT license

	frameworks and systems without the need for custom development		
PHPComplex (3.0.1)	PHP Class Library for working with Complex numbers Note: Required by phpspreadsheet	/vendor/markbaker/complex	MIT license
PHPMailer (v6.6.0)	The classic email sending library for PHP	/vendor/phpmailer/phpmailer	LGPL-2.1 license
PHPMatrix (3.0.0)	PHP Class for handling Matrices Note: Required by phpspreadsheet	/vendor/markbaker/matrix	MIT license
PhpSpreadsheet (1.19.0)	A pure PHP library for reading and writing spreadsheet files	/vendor/phpoffice/phpspreadsheet	MIT license
Riak Client (3.4.3)	PHP clients for Riak Note: Required by simplesamlphp	/vendor/phpfastcache/riak-client	Apache-2.0 license
Select2 (4.1.0-beta.1)	Select2 is a jQuery based replacement for select boxes.	/js/select2.min.js	MIT license
Selectize.js (v0.13.6)	Selectize is the hybrid of a textbox and <select> box.	/vendor/simplerisk/selectize.js	Apache-2.0 license
SimpleSAMLphp (v1.19.5)	SimpleSAMLphp is an award-winning application written in native PHP that deals with authentication.	/vendor/simplesamlphp/simplesamlphp	LGPL-2.1, Unknown licenses found
SortTable (version 2, 7th April 2007)	Make all your tables sortable	/js/sorttable.js	X11 licence
Swagger PHP	Generate interactive OpenAPI documentation for your RESTful API using doctrine annotations.	/vendor/zircote/swagger-php	Apache License 2.0

Swagger UI	Swagger UI allows anyone — be it your development team or your end consumers — to visualize and interact with the API's resources without having any of the implementation logic in place.	/vendor/swagger-api/swagger-ui	Apache License 2.0
Swift Mailer (v6.3.0)	Swiftmailer will stop being maintained at the end of November 2021. Please, move to Symfony Mailer at your earliest convenience. Note: Required by Jobby	/vendor/swiftmailer/swiftmailer	MIT license
Symfony	The Symfony PHP framework Note: Required by Jobby. Reliance on PHP >= 7.2 prevents upgrading.	/vendor/symfony	MIT license
TinyMCE (6.0.0)	The world's #1 JavaScript library for rich text editing.	/vendor/tinymce/tinymce	MIT license
Twig (v2.15.2)	Twig is a template language for PHP. Note: Required by simplesamlphp	/vendor/twig/twig	BSD-3-Clause license
Underscore (1.13.2)	JavaScript's utility _ belt	/vendor/components/underscore	MIT license
Webmozart Assert (1.11.0)	Assertions to validate method input/output with nice error messages. Note: Required by simplesamlphp	/vendor/webmozart/assert	MIT license
Xmlseclibs (3.1.1)	A PHP library for XML Security Note: Required by simplesamlphp	/vendor/robrichards/xmlseclibs	BSD-3-Clause license

ZipStream-PHP (2.1.0)	PHP ZIP Streaming Library Note: Required by phpspreadsheet. Reliance on PHP >= 7.2 prevents upgrading beyond 2.1.0. Current version is 2.2.1.	/vendor/maennchen/zipstream-php	MIT license

Dependency Notes

- **Duo PHP:** This library was used for Duo MFA as part of the Custom Authentication Extra. Its use has been deprecated as of the 20230106-001 release with the inclusion of google2fa in the SimpleRisk Core and will eventually be completely removed.
- **Epiphany:** This library is used as a core component of the SimpleRisk API functionality. This is considered a medium priority since the attack surface is minimal and there are no known vulnerabilities, but we recognize that this dependency will need to eventually be replaced or forked to be supported by us.
- **Swift Mailer:** This library stopped being maintained at the end of November 2021. It is not used by SimpleRisk directly, but rather included by the Jobby library that we use. We are actively tracking their response to this issue here.
- **Bootstrap Multiselect:** The original website where this file points to no longer hosts this content. Unsure if this is the latest version. We should consider replacing it with a different multiselect library.
- **Color picker:** This is not the latest version of color picker available and we should look to upgrade to the 23.05.2009 version or consider replacing it with another library.
- **CSRF-Magic:** As the original CSRF-Magic library is no longer supported, we have forked this library under our control.
- **Datatables:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **Date Range Picker:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **EasyUI for jQuery:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **jQuery BlockUI:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **jQuery DateTimePicker:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **Laminas ZendFramework Bridge:** Required by Laminas Escaper. Managed via Composer, but a reliance on PHP >= 7.2 prevents upgrading beyond 1.1.1. Current version is 1.6.1.
- **PHP Enum:** Required by zipstream-php. Managed via Composer, but a reliance on PHP >= 7.2 prevents upgrading beyond 1.7.7. Current version is 1.8.4.
- **Select2:** As this is in the /js directory, it must be managed manually and regularly checked for updates.

- **Selectize.js:** This library is still actively supported, but we forked it so that it could be included and regularly updated via Composer.
- **SortTable:** As this is in the /js directory, it must be managed manually and regularly checked for updates.
- **Symfony:** Required by Jobby. Managed via Composer, but a reliance on PHP >= 7.2 prevents upgrading.
- **ZipStream-PHP:** Required by phpspreadsheet. Managed via Composer, but a reliance on PHP >= 7.2 prevents upgrading beyond 2.1.0. Current version is 2.2.1.

Control Frameworks Included in the SimpleRisk Core

- CIS Critical Security Controls: Verified with CIS that can be included in SimpleRisk.
- HIPAA (April 2016): Unsure of license status.
- NIST 800-171 : Publication is free of charge.
- PCI DSS 3.2: Unsure of license status.
- PCI DSS 4.0: Unsure of license status.

SimpleRisk Extras: These are the paid-for plug and play additions to the SimpleRisk Core. These may be individually licensed or purchased as a package. Terms and conditions vary by customer as well as deployment scenario.

Control Frameworks Included in SimpleRisk Extras

- Secure Controls Framework: Included in the Secure Controls Framework (SCF) Extra. Licensed under the Creative Commons Attribution-NoDerivatives 4.0 International Public License.