OWASP Dependency-Check Plugin

Plugin Information

View OWASP Dependency-Check on the plugin site for more information.

Older versions of this plugin may not be safe to use. Please review the following warnings before using an older version:

- Persisted cross-site scripting vulnerability

This plugin can analyze dependencies and generate trend reports for Dependency-Check, an open source utility that detects known vulnerabilities in project dependencies.

Description

Dependency-Check is an open source utility that identifies project dependencies and identifies if there are any known, publicly disclosed, vulnerabilities. This tool can be part of the solution to the OWASP Top 10: Using Components with Known Vulnerabilities.

The Dependency-Check Jenkins Plugin features the ability to perform a dependency analysis build and later view results post build.

Usage

The plugin has three main components: a globally defined tool configuration, a builder, and a publisher.

Global Tool Configuration

One or more Dependency-Check versions can be installed via the Jenkins Global Tool Configuration. The installation of Dependency-Check can be performed automatically, which will download and extract the official Command-Line Interface (CLI) from Bintray, or an official distribution can be installed manually and the path to the installation referenced in the configuration.

Builder

The builder performs an analysis using one of the pre-defined Dependency-Check CLI installations. Configuration specific to Jenkins is minimal, with important aspects of the job configuration being the ‘Arguments’ field, which is sent directly to the CLI installation defined.
Publisher

The publisher works independently of the tool configuration or builder and is responsible for reading dependency-check-report.xml and generating metrics, trends, findings, and optionally failing the build or putting it into a warning state based on configurable thresholds.

Risk Gate Thresholds

<table>
<thead>
<tr>
<th>Total Findings</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Warning.png" alt="Warning Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Findings</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Warning.png" alt="Warning Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
<td><img src="Status.png" alt="Status Icon" /></td>
</tr>
</tbody>
</table>

When a job has the publisher configured, a trending chart will display the total number of findings grouped by severity.
The chart is interactive. Hovering over a build will display high-level severity information.

Per-build results may be viewed. Findings are displayed in an interactive table which can be sorted, searched on, and paginated through. Each findings can be expanded to reveal additional details.
Version History

Version 5.0.1 (July 8, 2019)
- Fixed issue in publisher which prevented the saving and use of XML report patterns other than the default
- Added check to publisher which puts build into warning state if no reports are found

Version 5.0.0 (July 7, 2019)
- Complete rewrite ported from OWASP Dependency-Track Plugin
- Utilizes Jenkins Global Tool Configuration and automatically installs Dependency-Check CLI if necessary
- Multiple versions of Dependency-Check can be executed at the same time
- Jobs can be configured to always use the latest version of Dependency-Check, or can specify exactly which version to use
- Jenkins plugin will no longer need updating upon every Dependency-Check release. It now has an independent release schedule
- Jobs now have full control over every configurable option
- Publisher parses Dependency-Check XML reports generated from Dependency-Check v5.0 and higher
- Dynamic and interactive trends and results
- Not compatible with previous versions (refer to v5 migration wiki)

Version 4.0.2 (January 1, 2019)
- Updated core to Dependency-Check v4.0.2

Version 4.0.1 (December 17, 2018)
- Added support for non-proxy hosts as defined in the Jenkins proxy settings
- Updated core to Dependency-Check v4.0.1

Version 4.0.0 (November 21, 2018)
- Updated core to Dependency-Check v4.0.0

Version 3.3.4 (October 28, 2018)
- Updated core to Dependency-Check v3.3.4

Version 3.3.3 (October 27, 2018) - NOT RELEASED
- Removed support for legacy NSP analyzer
- Added support for Node Audit analyzer
- Updated core to Dependency-Check v3.3.3
- Minor corrections to parser (vulnerability source) and jelly templates
Version 3.3.2 (September 16, 2018)

- Updated core to Dependency-Check v3.3.2

Version 3.3.1 (August 6, 2018)

- Added NuGet config analyzer
- Updated core to Dependency-Check v3.3.1

Version 3.3.0 (July 23, 2018)

- Added Artifactory, MSBuild Project, and Retire.js analyzers
- Added plugin as a 'buildPlugin' for Jenkins pipeline
- Corrected issue that may have caused the number of new and fixed issues to be reported incorrectly
- Fixed issue with Dependency-Track publisher that failed if artifact was blank
- Fixed internal issue with Engine closing
- Updated core to Dependency-Check v3.3.0

Version 3.2.1 (May 28, 2018)

- Updated core to Dependency-Check v3.2.1

Version 3.2.0 (May 21, 2018)

- Updated core to Dependency-Check v3.2.0
- Updated analysis-core to v1.94
- Updated token-macro to v2.1

Version 3.1.2.1 (May 2, 2018)

- Fixed issue that resulted in the Dependency-Track publisher failing on slave nodes
- Enhanced online help when configuring jobs which describes permissions required in Dependency-Track
- Relaxed URL format for Dependency-Track. Will ignore trailing slash if present.

Version 3.1.2 (April 2, 2018)

- Updated core to Dependency-Check v3.1.2
- Added links to CWEs in report console
- Added additional links to CVEs in fixed and warnings tabs
- Added option to disable Node Package Manager analyzer

Version 3.1.1 (January 28, 2018)

- Updated core to Dependency-Check v3.1.1
- Updated Jenkins parent to use modern pom (thanks CloudBees)
- Updated Java version requirement to Java 8
- Added software bill-of-material (CycloneDX and SPDX) support to Dependency-Track publisher

Version 3.1.0 (January 4, 2018)

- Disabled Ruby Bundler Analyzer by default
- Fixed issue that prevented publishing to Dependency-Track when project did not have a version
- Updated core to Dependency-Check v3.1.0
- Updated analysis-core to v1.88
- Minor spelling and labeling changes

Version 3.0.2 (November 14, 2017)

- Updated core to Dependency-Check v3.0.2

Version 3.0.1 (October 19, 2017)

- Updated core to Dependency-Check v3.0.1

Version 3.0.0 (October 15, 2017)

- Fixed serialization issue that prevented Dependency-Track Publisher from running on slave nodes
- Removed legacy Node.js analyzer
- Updated core to Dependency-Check v3.0.0


- Added Groovy syntax support when defining pipeline jobs
- Fixed defect that prevented pipeline execution from properly executing on slave nodes
* Updated core to Dependency-Check v2.1.1

Version 2.1.0 (July 23, 2017)
* Updated core to Dependency-Check v2.1.0

Version 2.0.1.2 (July 20, 2017)
* Fixed XSS vulnerability - SECURITY-577

Version 2.0.1.1 (July 10, 2017)
* Fixed defect that caused NPE when the publisher step parsed Dependency-Check XML reports containing suppressions

Version 2.0.1 (July 6, 2017)
* Updated core to Dependency-Check v2.0.1

Version 2.0.0 (July 3, 2017)
* Updated core to Dependency-Check v2.0.0
* Updated analysis-core to v1.86
* Added support for Node Security Platform
* Added Jenkins Pipeline support to all builders
* Added finer control over optional HTML, JSON, and CSV reports to generate
* Added ability to publish Dependency-Check results to Dependency-Track v3
* Enhancements to user interface
* Fixed bug that prevented updateOnly builder from using external database
* Fixed bug that failed to mask password when using external database

Version 1.4.5 (January 23, 2017)
* Updated core to Dependency-Check v1.4.5
* Updated analysis-core to v1.80
* Minor modifications to Python configuration
* Added support for Ruby Bundler analyzer
* Added support for hints file
* Fixed null pointer exception

Version 1.4.4 (November 5, 2016)
* Updated core to Dependency-Check v1.4.4
* Added global data directory option (with local override)
* Fixed null pointer exception

Version 1.4.3 (September 6, 2016)
* Updated core to Dependency-Check v1.4.3
* Added CocoaPods analyzer support
* Added Swift Package Manager analyzer support

Version 1.4.2 (July 31, 2016)
* Updated core to Dependency-Check v1.4.2

Version 1.4.1 (July 31, 2016)
* Updated core to Dependency-Check v1.4.1
* Updated analysis-core to v1.79
* Java 7 or higher is now a requirement - Version checking implemented
* Corrected description in verbose logging help
* Added XSS prevention missing on three files

Version 1.4.0 (June 16, 2016)
* Separated out standard and experimental analyzers in global config
* Added optional external database configuration options to global config
* Updated core to Dependency-Check v1.4.0
* Updated analysis-core to v1.78

Version 1.3.6 (April 10, 2016)
* Updated core to Dependency-Check v1.3.6
Version 1.3.5 (March 5, 2016)
- Updated core to Dependency-Check v1.3.5
- Updated analysis-core to v1.76

Version 1.3.4 (February 1, 2016)
- Updated core to Dependency-Check v1.3.4
- Updated analysis-core to v1.75

Version 1.3.3 (December 11, 2015)
- Updated core to Dependency-Check v1.3.3

Version 1.3.2 (November 29, 2015)
- Updated core to Dependency-Check v1.3.2

Version 1.3.1.2 (November 13, 2015)
- Fixed relative (to workspace) path resolution for suppression files

Version 1.3.1.1 (November 10, 2015)
- Fixed regression that prevented suppression files from being honored

Version 1.3.1 (September 21, 2015)
- Added RubyGem analyzer support
- Added PHP Composer lock analyzer support
- Added Node.js analyzer support
- Added support for Jenkins Workflow plugin (thanks CloudBees)
- Removed Javascript analyzer support
- Updated dashboard-view plugin to 2.9.6
- Updated analysis-core to v1.74
- Updated core to Dependency-Check v1.3.1

Version 1.3.0 (August 5, 2015)
- Added Autoconf analyzer support
- Added CMake analyzer support
- Added OpenSSL analyzer support
- Added QuickQuery Timestamp option to global config
- Added support for token-macro plugin
- Added support for dashboard-view plugin
- CVSS attributes now popup when hovering over CVSS score in details view
- Updated analysis-core to v1.72
- Updated core to Dependency-Check v1.3.0
- Bug fixes

Version 1.2.11.1 (June 10, 2015)
- Fixed defect introduced in 1.2.11 that prevented execution on slave nodes

Version 1.2.11 (May 12, 2015)
- Added Python analyzer support
- Added new builder (build step) that can perform an NVD update only
- Updated analysis-core to v1.71
- Updated core to Dependency-Check v1.2.11
- Minor refactoring to minimize DRY

Version 1.2.10 (April 12, 2015)
- Updated core to Dependency-Check v1.2.10

Version 1.2.9 (March 6, 2015)
- Updated core to Dependency-Check v1.2.9
- Added warning if the Maven Central or Nexus analyzer are disabled
- Added option to bypass Jenkins proxy configuration when downloading NVD feed
- Updated analysis-core to v1.69
- Changed label names on tabs
Version 1.2.8 (December 28, 2014)
- Updated core to Dependency-Check v1.2.8
- Minor code cleanup

Version 1.2.7.1 (December 28, 2014)
- Reverted previous serialization changes

Version 1.2.7 (December 8, 2014)
- Updated core to Dependency-Check v1.2.7
- Optimized serialization required for slave execution

Version 1.2.6 (November 16, 2014)
- Updated core to Dependency-Check v1.2.6
- Updated analysis-core to v1.65
- Added support for Maven Central analyzer

Version 1.2.5 (September 16, 2014)
- Updated core to Dependency-Check v1.2.5
- Support for Ant-style patterns added to scan path configuration

Version 1.2.4 (August 5, 2014)
- Updated core to Dependency-Check v1.2.4

Version 1.2.3.2 (July 7, 2014)
- Refactored experimental Maven artifact analysis
- Fixed display issued on details tab that may display incorrect path

Version 1.2.3.1 (July 1, 2014)
- Fixed UI defect that prevented plugin from being configured in some circumstances

Version 1.2.3 (June 27, 2014)
- Updated core to Dependency-Check v1.2.3

Version 1.2.2 (June 23, 2014)
- Updated core to Dependency-Check v1.2.2
- Updated analysis-core to v1.57
- Added experimental support for Maven artifact analysis in Maven jobs
- Added global configuration for analyzers and temporary directory

Version 1.2.1 (May 10, 2014)
- Updated core to Dependency-Check v1.2.1

Version 1.2.0 (April 28, 2014)
- Updated core to Dependency-Check v1.2.0
- Fixed defect that could result in a circular dependency

Version 1.1.4.1 (April 15, 2014)
- 1.1.4 did not release properly due to bug in Maven Release Plugin. This is a re-release of 1.1.4 using M-R-P v2.5

Version 1.1.4 (March 30, 2014)
- Updated core to Dependency-Check v1.1.4
- Updated analysis-core to v1.56
- Added URL support for suppression files
- Fixed bug that prevented workspace from being cleaned up due to H2 lock files in use
- Fixed defect in details view that prevented certain details from displaying if a CWE was not associated with a vulnerability
- Default filename for XML reports has changed

Version 1.1.3 (March 11, 2014)
- Updated core to Dependency-Check v1.1.3
Version 1.1.2 (March 3, 2014)
- Updated core to Dependency-Check v1.1.2
- Updated analysis-core to v1.55
- Added per-build configurable support for additional zip extensions
- Added global Nexus analyzer proxy bypass setting
- Added global Mono path configuration

Version 1.1.1.2 (February 9, 2014)
- Added per job configurable option to skip Dependency-Check analysis if job is triggered by an upstream change

Version 1.1.1.1 (February 8, 2014)
- Added per job configurable option to skip Dependency-Check analysis if job is triggered by SCM change

Version 1.1.1 (January 30, 2014)
- Updated core to Dependency-Check v1.1.1

Version 1.1.0 (January 26, 2014)
- Updated core to Dependency-Check v1.1.0
- Changed license from GPLv3 to Apache 2.0

Version 1.0.8 (January 18, 2014)
- Updated core to Dependency-Check v1.0.8
- Added global configuration options for Nexus analyzer
- Removed restriction that confined data directory to workspace
- Support for shared data directory (per node)

Version 1.0.7 (December 3, 2013)
- Updated core to Dependency-Check v1.0.7
- Added support for suppression file in build step

Version 1.0.6 (not published)

Version 1.0.5 (November 16, 2013)
- Updated core to Dependency-Check v1.0.5
- Updated analysis-core to v1.54
- Added support for proxy authentication
- Fixed bug that allowed a build to pass if invalid scan path was specified

Version 1.0.4.1 (October 31, 2013)
- Added ability to use mirrored NIST CPE/CVE data. Refer to nist-data-mirror for a simple tool to mirror NIST data
- Added partial proxy server support. The core currently supports hostname and port parameters

Version 1.0.4 (October 22, 2013)
- Updated core to Dependency-Check v1.0.4
- Added configurable option to enable verbose logging when using the build step

Version 1.0.3 (October 14, 2013)
- Updated core to Dependency-Check v1.0.3
- Added configurable option to generate standalone HTML reports in output directory

Version 1.0.2 (September 4, 2013)
- Updated core to Dependency-Check v1.0.2

Version 1.0.1.1 (August 30, 2013)
- Removed unnecessary dependency that may cause classpath issues

Version 1.0.1 (August 2, 2013)
- Initial public release
Sponsors

Development of Dependency-Check Jenkins Plugin prior to v3.0.3 was sponsored in part by Axway.