CAST Report Generator - Release Notes - 1.11.x

> (i) **Summary**: this page describes the new features and bugs that have been fixed in the CAST Report Generator 1.11.x.

Content matrix

Version	Summary of content	Comments
1.11.0		Can be used with: • CAST-RESTAPI 1.11.x

Component documentation

- CAST Report Generator - Components documentation - 1.11.0
  - CAST Report Generator - Text components available - 1.11.0
  - CAST Report Generator - Graph components - 1.11.0
  - CAST Report Generator - Table components - 1.11.0
  - CAST Report Generator - Generic components - 1.11.0

Resolved issues

N/A.

New templates

The following templates are new in v. 1.11.x:

- CISQ Compliance Report v2.docx
- CISQ Security Compliance Report.docx
- CWE Compliance Report.docx
- NIST-SP800-53R4 Compliance Report.docx
- PCI-DSS-V3.1 ComplianceReport.docx
- STIG V4R8 Standards-DetailedReport.docx
- STIG V4R8 Standards Compliance Report.docx

(i)

New components for templates

REPORTGEN-596 - QUALITY_TAGS_RULES_EVOLUTION

This component is new in v. 1.11.0 and displays the evolution of CAST rules associated to a quality standard category:

- Block Name = **QUALITY_TAGS_RULES_EVOLUTION**
- Options:
  - **STD=** Name of the quality standard category for which you want the details per tag, for example, STIG-V4R8-CAT1 will list total, added and removed violations for CAST rules associated to all tags belonging to category STIG-V4R8-CAT1.
  - **LBL= Violations** or **vulnerabilities** (vulnerabilities if not set) - this changes the headers from Vulnerabilities to Violations

Click to enlarge

STIG-V4R8-CAT1	Total Vulnerabilities	Added Vulnerabilities	Removed Vulnerabilities
STIG-V-70205 The application must not expose session IDs.	0	0	0
Avoid using HttpServletRequest.getRequestedSessionId()	0	0	0
STIG-V-70207 The application must destroy the session ID value and/or cookie on logoff or browser close.	0	0	1
Ensure that HTTP Session is invalidated during logout	0	0	1
STIG-V-70245 The application must protect the confidentiality and integrity of transmitted information.	4	0	0
Avoid mixing trusted and untrusted data in HTTP requests	0	0	0
Avoid providing password in Web Service URL	0	0	0
Avoid using RSA Cryptographic algorithms without OAEP (Optimal Asymmetric Encryption Padding)	0	0	0
Avoid using Deprecated SSL protocols to secure connection	0	0	0
Avoid using predictable SecureRandom Seeds	0	0	0
Avoid using risky cryptographic hash (JEE)	3	0	0
Avoid using Cipher with no HMAC to ensure data integrity	1	0	0
Avoid weak encryption providing not sufficient key size (JEE)	0	0	0

Notes:

- To use the quality standard tags selection with this component, the Quality Standards Mapping extension (with minimum version 20190624) should be installed on the Dashboard Service schema where the application resides.
- See CAST Report Generator - Table components - 1.11.0.

Changes to existing components for templates

REPORTGEN-541 - RULES_LIST_STATISTICS_RATIO

This component has been changed to add the **EVOLUTION** option:

- **EVOLUTION=true|false** to display added and removed violations columns. By default or if not exists, is true (to keep compatibility with old version)

See CAST Report Generator - Table components - 1.11.0.

REPORTGEN-566 - REMOVED_VIOLATIONS_LIST

This component has been changed to add the **CRITICITY** option:

- **CRITICITY = c** for "only critical violations", **nc** for "only non-critical violations", **all** for critical and non-critical violations (**all** by default if not configured)

Examples:

- all critical violations deleted for Business Criterion "Robustness": **TABLE;REMOVED_VIOLATIONS_LIST;BCID=60013,COUNT=-1,CRITICITY=c**
- first 50 non-critical violations deleted for TQI: **TABLE;REMOVED_VIOLATIONS_LIST;BCID=60017,COUNT=50,CRITICITY=nc**
- first 50 violations deleted for Business Criterion "Changeability" (critical and non critical): **TABLE;REMOVED_VIOLATIONS_LIST;BCID=60012, COUNT=50,CRITICITY=all**

See CAST Report Generator - Table components - 1.11.0.

REPORTGEN-571 - LIST_RULES_VIOLATIONS_BOOKMARKS and QUALITY_RULE_VIOLATIONS_BOOKMARKS

These two components have been updated as follows: when there is an associated value of integer type, this value is also displayed. See CAST Report Generator - Table components - 1.11.0.

REPORTGEN-596 - QUALITY_STANDARDS_EVOLUTION

This component has been changed to add the **MORE** option:

- **MORE=true** : add this if you have specified a category in STD and want the evolution of the tags associated to this category (not specified by default)

This option is valuable only when STD is a category (for example category = STIG-V4R8, tag = STIG-V4R8-CAT1). For a tag, there is no more data and the display is worse (for example tag = OWASP-2017 for which category=OWASP). See CAST Report Generator - Table components - 1.11.0. For example:

STIG-V4R8	Total Vulnerabilities	Added Vulnerabilities	Removed Vulnerabilities
STIG-V4R8-CAT1	**0**	**0**	**0**
STIG-V-70245 The application must protect the confidentiality and integrity of transmitted information.	0	0	0
STIG-V-70261 The application must protect from command injection.	0	0	0
STIG-V4R8-CAT3	**589**	**31**	**6**
STIG-V-70385 The application development team must follow a set of coding standards.	589	31	6

Table 2: STIG V4R8 summary

Updates

REPORTGEN-565 - Ability to use Report Generator with a CAST dashboard/RestAPI deployed with SAML authentication

If you have enabled SAML authentication mode for your CAST Dashboard/RestAPI deployment, Report Generator will not be able to authenticate to access data. This is because SAML is designed as a single sign-on mode for browsers and therefore non-browser clients (like Report Generator) cannot use the protocol. In order to resolve this issue, CAST provides the ability to define an **API Key** in the CAST dashboards/RestAPI that can be used to bypass SAML authentication.

How does this work?

- SAML authentication mode is enabled and configured for your CAST dashboard/RestAPI deployment
- In addition, an **API Key** is defined in the **security.properties** file in your CAST dashboard/RestAPI deployment
- The **API Key** is used instead of a **password**
- Clients must use two specific HTTP headers to ensure that the API Key is used (**Report Generator GUI** is pre-configured to send these headers, Report Generator CLI must use specific CLI options)
    - **X-API-KEY**: the API Key matching the key defined in the **security.properties** file
    - **X-API-USER**: a defined user name to obtain a CAST dashboard/RestAPI role and data authorization

- When an API Key is used to bypass SAML mode, the user will be automatically granted the **"ADMIN" role** even if this role has not explicitly been granted to the user in question.

You can find out more about this in CAST Dashboard Package - RestAPI authentication using an API key. To use the API key, you can define it in the **GUI** or via the **command line** (both the traditional Windows version and the cross-platform CAST Report Generator for Dashboards version). See the following documentation for more information:

GUI

- Configuring access to the data

CLI

- CAST Report Generator - CAST Report Generator for Dashboards
- Command line interface

REPORTGEN-572 - Obsolete templates removed and renamed

The following obsolete templates are no longer delivered with Report Generator:

- 2- Word-components-library.docx
- Portfolio/2- Portfolio-Word-components-library.docx

These templates have equivalent newer versions that have been delivered with Report Generator for some time (with the word "new" in the template title). Therefore the newer templates have been renamed to match the names of the removed templates. See CAST Report Generator - Templates and output options.