Changes in results post upgrade - 8.3.26

Summary: this page lists:

- Impacts of changes made to CAST AIP 8.3.26 on Quality Model results post upgrade
- Other impacts of changes made in CAST AIP 8.3.26

All changes in results related to extensions are now listed in the extension documentation and will not appear in this page.

Impacts of changes made in CAST AIP 8.3.26 on Quality Model results post upgrade

Avoid SQL injection vulnerabilities - 7742

Due to new support introduced in 8.3.26 for the framework **Microsoft.Practices.EnterpriseLibrary** by the **User Input Security** feature, results for the rule **Avoid SQL injection vulnerabilities** may change after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code - a decrease in the number of false violations may be visible.

Avoid file path manipulation vulnerabilities - 7752

A bug has been discovered in the User Input Security analysis which is causing false positive violations to be reported for **Avoid file path manipulation vulnerabilities** in .NET source code. This was due to a bug where the analyzer was programmed to record that the **New System.IO.StreamReader** for the entry-point opened a file and therefore declares a path manipulation causing a violation of the rule. This bug has been fixed and after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: less violations of this rule providing more accuracy.

Avoid use of a reversible one-way hash - 8416

User Input Security now detects violations for the rule **Avoid use of a reversible one-way hash** in .NET source code. Previously, only JEE source code was supported. Therefore after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: additional violations of this rule providing more accuracy.

Avoid using hard-coded HMAC keys - 8424

A bug has been discovered where the CAST Engineering Dashboard was reporting a Total Checks value less than the number of objects in violation (Total Checks should never be less than the number of objects in violation). This was caused by a bug in the rule algorithm where some items were missing from the rule scope. This bug has been fixed, therefore after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: Total Checks should be equal to or greater than the number of objects in violation.

Never truncate data in MOVE statements - 7688

A bug has been discovered which is causing false positive violations to be reported for **Never truncate data in MOVE statements**. This bug has been fixed and after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: less violations of this rule providing more accuracy.

User Input Security - new rules

The following new rules have been implemented, therefore after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: additional violations may be visible for these new rules:

Rule ID	CWE ID	Rule name	Input name	Target name	.NET support	JEE support
8518	400	Regular expression injection	Network.read	Regexp.write	Partial	NO
8520	400	Regular expression injection (second order)	Network.readDatabase	Regexp.write	Partial	NO
8522	400	Regular expression injection through API	Network.readAPI	Regexp.write	Partial	NO

Other impacts of changes made in CAST AIP 8.3.26

Mainframe

Updates to Base_Mainframe.TCCSetup for transaction configuration

The following changes have been implemented which may impact results when re-analyzing an existing application with AIP 8.3.26:

- IMS Transactions are now automatically considered part of "Standard Entry Point - IMS - Unknown (GS)"
- CICS Transactions called from Java methods and Java constructors are no longer considered part of "Standard End Point - CICS - Transactions called by Java (GS)"
- An error has been fixed where the opposite was true in previous releases:
    - IMS FilePrototype objects are now considered part of "Standard End Point - IMS - GSAM - Not delivered"
    - IMS AnalyzedFileobjects are now considered part of "Standard Data Entity - GSAM"

Name of unresolved MQ publisher/subscriber objects has been changed to avoid false links

In previous releases of AIP, unresolved queue names lead to the creation of Publisher/Subscriber objects with the same name **Unresovled:MQP2P**. As a result, many false links are created skewing results. In CAST AIP 8.3.26, the name of the unresolved object has been changed from **Unresolved:MQP2P** to **UnknownMQ:<COBOL_Parent_PROGRAM>** - this identifies the Cobol program name publishing/subscribing to the message and will reduce the number of false links. This may impact results when re-analyzing an existing application with AIP 8.3.26.

Update to ensure JCL SQL Query objects are created correctly

A change has been implemented to ensure that JCL SQL Query objects are created correctly when the DSNTIAUL program is used. This may impact results when re-analyzing an existing application with CAST AIP 8.3.26.

CAST Transaction Configuration Center

Improved accuracy of AETP values

In order to provide greater accuracy, the calculation of AETP values has been modified in this release. Previously, all added/deleted/updated AETP detail values between 0 and 1 were calculated with no decimal places, effectively giving the impression in some circumstances (when all added/deleted/updated values were below 1) that total AETP = 0. This behaviour has been changed and AETP detail values are now considered to two decimal places for added /deleted/updated. In addition AETP total values will now be **rounded up.** As a result of this change, some impact to results may be evident after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code: AETP values may change and as a result overall AEP values may also change.

User Input Security

A bug has been discovered in the implementation of the support for the **resthub-web-client-2.2.0** framework (introduced in **CAST AIP 8.3.25**). Some methods were not taken into account due to the way in which the support was programmed. As a result of this change, after an upgrade to 8.3.26 and the generation of a consistency snapshot on unchanged source code, results may change: potentially more violations on methods that were not taken into account in previous analyses.