

# Changes or new features - 8.3.28 and above

--

- 8.3.37
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.36
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.35
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.34
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.33
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.32
  - New Features
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.31
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.30
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.29
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.28
  - Feature Improvements
- 8.3.27
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.26
  - Feature Improvements
  - Resolved Issues
- 8.3.25
  - Note
  - Feature Improvements
  - Other Updates
  - Resolved Issues
- 8.3.24
  - Feature Improvements
  - Resolved Issues
- 8.3.23
  - Note
  - Feature Improvements
  - Resolved Issues
- 8.3.22
  - Feature Improvements
  - Resolved Issues
- 8.3.21
  - Feature Improvements
  - Resolved Issues
- 8.3.20
  - Feature Improvements
  - Resolved Issues
- 8.3.19
  - Feature Improvements
  - Resolved Issues
- 8.3.18
  - Feature Improvements
  - Resolved Issues
- 8.3.17
  - Feature Improvements
  - Resolved Issues
- 8.3.16
  - Feature Improvements
  - Resolved Issues

 **Summary:** This page lists all changes provided in AIP 8.3.28 and above.

## 8.3.37

### Feature Improvements

Summary	Details
.NET Discoverer: improvements for the Nuget Resources Extractor	Improvements have been made to the .NET discoverer, embedded in AIP Core. These improvements are designed to allow additional packages to be considered by any release of the Nuget Resources Extractor (com.castsoftware.dmdotnetnugetresourcesextractor): packages referenced in the "packages.config" file (if delivered with the source code) will now be extracted and resolved (previously packages referenced in this file were ignored). This change may impact previous analysis results if upgrading to AIP Core 8.3.37 (or future releases): additional packages may be extracted that were previously ignored.
Improve results for "Lack of Cohesion" type rules	In an effort to improve the results and reduce the number of false positives returned by the rules "Avoid Classes with a High Lack of Cohesion" (7798) and "Avoid Classes with a High Lack of Cohesion variant" (7796), the scope of both rules has been modified. Starting AIP Core 8.3.37, only classes with at least one field and more than one method will form the scope of objects considered for these two rules. As a result of this change to the scope, existing analysis results may be impacted when upgrading to AIP Core 8.3.37 and running a new analysis with unchanged source code. See <a href="https://doc.castsoftware.com/display/AIPCORE/Changes+in+results+post+upgrade+-+8.3.37#Changesinresultspostupgrade8.3.37-AvoidClasseswithaHighLackofCohesion(7798)andAvoidClasseswithaHighLackofCohesionvariant(7796)">https://doc.castsoftware.com/display/AIPCORE/Changes+in+results+post+upgrade+-+8.3.37#Changesinresultspostupgrade8.3.37-AvoidClasseswithaHighLackofCohesion(7798)andAvoidClasseswithaHighLackofCohesionvariant(7796)</a> .
User Input Security: improvements to the rule "Avoid weak cryptographic algorithm" (8414) for .NET	The rule "Avoid weak cryptographic algorithm" (8414) for .NET has been improved to detect violations for "constructor call" targets for the System.Security.Cryptography API. This improvement may impact existing results - additional violations may be detected.

### Other Updates

Internal Id	Details
AIPCORE-3279	Change of use for CTT_OBJECT_APPLICATIONS table in Analysis schema: if you are using this table in a "Tools after module generation" SQL Tool job in the CAST Management Studio to create a custom exclusion of objects from the Dashboard schema (and therefore from the Engineering Dashboard), then you must update your scripts. The previous method was to use "set PROPERTIES = 1" on a specific OBJECT_ID which marked the object as external, therefore excluding it from the Dashboard schema. Starting AIP Core 8.3.37 you must instead use "set PROPERTIES = PROPERTIES   256" to exclude the object.
AIPCORE-3445	Fixes have been applied to prevent the number of Total Checks (displayed in the Engineering Dashboard) for specific rules triggered by the User Input Security feature (for .NET and JEE) exceeding the total number of violations reported. See also <a href="https://doc.castsoftware.com/display/AIPCORE/Changes+in+results+post+upgrade+-+8.3.37#Changesinresultspostupgrade8.3.37-TotalChecksdiscrepancies">https://doc.castsoftware.com/display/AIPCORE/Changes+in+results+post+upgrade+-+8.3.37#Changesinresultspostupgrade8.3.37-TotalChecksdiscrepancies</a> .

### Resolved Issues

Customer Ticket Id	Details
29986	False positive for rule, "Avoid Open SQL SELECT queries without WHERE condition on XXL Tables".
28385	Mapped drive on Linux throws error when connecting to AIP console.
30210	Application name with special character such as ( ) will fail when running the upgrade batch script.
30549	Analysis fails with XMLTODB error during "Run dataflow security analysis".
30844	A fix has been provided in the CAST Database Extractor delivered with AIP Core for the following error reported during an extraction: "Oracle DB Extraction error: ORA-01555: snapshot too old: rollback segment number 237 with name "_SYSSMU237_676302553\$" too small".

30888	Right clicking on objects added to the Enlighten view causes Enlighten to crash.
28750	Empty web JSP analysis units are created in AIP Console.
29859	Violations are more than TOTAL checks for the rule "8240: Avoid using unsecured cookie".
30341	Object types are present in CAST Imaging even though their Analysis Units have been disabled and are not being analyzed.
30490	Object types are present in CAST Imaging even though their Analysis Units have been disabled and are not being analyzed.
30445	False violation for rule "Avoid Classes with a High Lack of Cohesion".
30840	Analysis failed with error: Duplicate key violates unique constraint "pk_objjnf".

## 8.3.36

### Feature Improvements

Summary	Details
User Input Security: New rule "Avoid using insufficient random generator" (8554)	A new non-critical rule called "Avoid using insufficient random generator" (8554) has been implemented for both JEE and .NET technologies. This rule is triggered when the User Input Security feature is enabled and contributes to the "Secure Coding - Weak Security Features" technical criterion (66064).
User Input Security: New rule "Avoid expression language injection" (8536)	A new non-critical rule called "Avoid expression language injection" (8536) has been implemented for JEE technology. This rule is triggered when the User Input Security feature is enabled and contributes to the "Secure Coding - Input Validation" technical criterion (66062).
User Input Security: improvements to the rule "Avoid weak cryptographic algorithm" (8414) for .NET	The rule "Avoid weak cryptographic algorithm" (8414) for .NET has been improved to detect violations for "create" targets on weak algorithms (such as "var md5 = MD5.Create();"). This improvement may impact existing results.
User Input Security: New rule "Avoid debug forging" (8542)	A new non-critical rule called "Avoid debug forging" (8542) has been implemented for both .NET and JEE technologies to target the use of "log.debug". This rule is triggered when the User Input Security feature is enabled and contributes to the "Secure Coding - Input Validation" technical criterion (66062).
ABAP: New rule "Avoid using ABAP command OPEN DATASET with the FILTER addition" (8552)	A new critical rule called "Avoid using ABAP command OPEN DATASET with the FILTER addition" (8552) has been implemented for ABAP technology. This rule contributes to the "Secure Coding - Input Validation" technical criterion (66062).
ABAP: New rule "Avoid using ABAP command INSERT REPORT" (8548)	A new critical rule called "Avoid using ABAP command INSERT REPORT" (8548) has been implemented for ABAP technology. This rule contributes to the "Secure Coding - Input Validation" technical criterion (66062).
ABAP: New rule "Avoid using ABAP command GENERATE SUBROUTINE POOL" (8550)	A new non-critical rule called "Avoid using ABAP command GENERATE SUBROUTINE POOL" (8550) has been implemented for ABAP technology. This rule contributes to the "Programming Practices - Structuredness" technical criterion (61024).
ABAP: New rule "Avoid using ABAP command CALL 'SYSTEM'" (8546)	A new critical rule called "Avoid using ABAP command CALL 'SYSTEM'" (8546) has been implemented for ABAP technology. This rule contributes to the "Secure Coding - Input Validation" technical criterion (66062).

### Other Updates

Internal Id	Details
AIPCORE-3292	User Input Security: the location of XSS target violations in .NET code detected by rules triggered by the User Input Security feature are now more precisely positioned in the Engineering Dashboard. Previously, violations which cover multiple code lines were not correctly positioned because the start and end line numbers of the violation in the code were identical.
AIPCORE-3277	User Input Security: As a result of the implementation of a new rule "Avoid debug forging" (8542) to specifically target the use of "log.debug", an existing rule "Avoid log forging" (8044), has been modified: this rule no longer detects the use of "log.debug". This change may impact existing results.

### Resolved Issues

Customer Ticket Id	Details
--------------------	---------

29410	VB analysis fails in AIP Console when the AIP Node package is running as a Windows Service using the LocalSystem account.
29568	VB analysis fails in AIP Console when the AIP Node package is running as a Windows Service using the LocalSystem account.
29748	Complexity Factor values for modified transactions: in previous releases of AIP Core, the Complexity Factor (CF) for a modified transaction was erroneously set to 0 when any artifact with complexity was involved in the changes. This bug resulted in an AEP value of 0 despite the fact that a transaction had been modified. This bug has now been corrected, and as per the specification (see <a href="https://doc.castsoftware.com/display/AIPCORE/CAST+Automated+Enhancement+Points+Estimation+-+AEP#CASTAutomatedEnhancementPointsEstimationAEP-ComplexityFactor">https://doc.castsoftware.com/display/AIPCORE/CAST+Automated+Enhancement+Points+Estimation+-+AEP#CASTAutomatedEnhancementPointsEstimationAEP-ComplexityFactor</a> ) the minimum Complexity Factor value for a modified transaction will be set to 0.25 in AIP Core 8.3.36 - this ensures that the AEP value will be impacted when an existing transaction is modified. This change will also be applied to existing results during an upgrade to AIP Core 8.3.36, and as result, any modified transaction with a Complexity Factor of 0 will be changed to 0.25. This change may impact other metrics and rules that rely on these values.
30045	Unable to run a CAST AIP Setup if the setup file has special characters in it.
29815	While packaging, in the discovery phase, following warning is displayed – “The format may not be supported, the file may be corrupted, or it may not be a C# or VB.NET project at all”.
29693	While running ABAP analysis for couple of files, following warning message is displayed: MemMngrDLL_FreeBlock(): There remain 'active' pointers on the current deleted user area of bytes.

## 8.3.35

### Feature Improvements

Summary	Details
Rules - Bookmarks for violations of the rule "Avoid Open SQL SELECT queries without WHERE condition on XXL Tables" (8464)	Bookmarks for violations of the rule "Avoid Open SQL SELECT queries without WHERE condition on XXL Tables" (8464) are not displayed. This behaviour has now been changed and bookmarks are now available for violations raised by this rule.
User Input Security - support for org.owasp.esapi framework.	The User Input Security feature now supports the JEE framework org.owasp.esapi. All "getValidate*" methods are now automatically taken into account as sanitization methods for all quality rules.
User Input Security - new rules to support the detection of XQuery Injections	Three new rules have been implemented for JEE and .NET technologies to support the detection of XQuery Injections: 1) "Avoid XQuery injection" (8530), 2) "Avoid second order XQuery injection" (8532), 3) "Avoid XQuery injection through API requests" (8534).
User Input Security - improved support for .NET UI controls for XSS violations	Improved support for .NET UI controls as targets for XSS violations has been implemented, for example "set_Text" and "set_ImageUrl" methods of control objects.

### Other Updates

Internal Id	Details
AIPCORE-3161	The title of the rule "Avoid file path manipulation vulnerabilities through API requests." (8506) has been changed to "Avoid file path manipulation through API requests ". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid XPath injection vulnerabilities through API requests." (8504) has been changed to "Avoid XPath injection through API requests ". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid thread injection vulnerabilities through API requests." (8498) has been changed to " Avoid thread injection through API requests ". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid OS command injection vulnerabilities through API requests." (8494) has been changed to "Avoid OS command injection through API requests". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid SQL injection vulnerabilities through API requests." (8490) has been changed to " Avoid SQL injection through API requests". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid thread injection vulnerabilities." (8436) has been changed to "Avoid thread injection". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid log forging vulnerabilities." (8044) has been changed to " Avoid log forging ". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid SQL injection vulnerabilities." (7742) has been changed to " Avoid SQL injection". There is no impact on existing results.

AIPCORE-3161	The title of the rule "Avoid LDAP injection vulnerabilities." (7746) has been changed to " Avoid LDAP injection". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid OS command injection vulnerabilities." (7748) has been changed to " Avoid OS command injection". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid XPath injection vulnerabilities." (7750) has been changed to "Avoid XPath injection". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid file path manipulation vulnerabilities." (7752) has been changed to "Avoid file path manipulation". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid Regular expression injection through API requests." (8522) has been changed to "Avoid regular expression injection through API requests". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid Regular expression injection." (8518) has been changed to " Avoid regular expression injection". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid second order Regular expression injection." (8520) has been changed to "Avoid second order regular expression injection". There is no impact on existing results.
AIPCORE-3237	A change has been made to the SAP discoverer. Previously, the discoverer would create only one single project (and therefore Analysis Unit) regardless of the number of SAP extractions provided in the source code delivery (it was assumed that only one extraction would be delivered). This behaviour has now been changed and multiple SAP extractions delivered in one go will result in one project (and therefore Analysis Unit) for each extraction. See also <a href="https://doc.castsoftware.com/display/TECHNOS/SAP+ABAP+Discoverer">https://doc.castsoftware.com/display/TECHNOS/SAP+ABAP+Discoverer</a> . This change may impact existing results.
AIPCORE-3161	The title of the rule "Avoid LDAP injection vulnerabilities through API requests" (8492) has been changed to "Avoid LDAP injection through API requests". There is no impact on existing results.
AIPCORE-3161	The title of the rule "Avoid log forging vulnerabilities through API requests" (8508) has been changed to "Avoid log forging through API requests". There is no impact on existing results.

## Resolved Issues

Customer Ticket Id	Details
29006	Incorrect violation for the rule, "Avoid unsorted data after SELECT queries - 8134".
29193	Java files are not analyzed when present in the "generated sources" folder.
29298	Restore_triplet step failed while adding application in Console 1.23.0, with the following error: cast combined importer.exe- unrecognized arguments
29332	There are six unsupported syntax warnings for different ABAP files. (ABAP analysis warning: ABAP.04: Unsupported syntax found at line).
29362	Discovery step during packaging fails with error, "java.lang.StackOverflowError"
29417	The SAP discoverer is creating one single package and one single Analysis Unit regardless of the number of extractions delivered in the source code. This behaviour has now been changed and multiple SAP extractions delivered in one go will result in one project (and therefore Analysis Unit) for each extraction.
29419	Warning during ABAP analysis: "processing listener CABAPFullParsingAction::processABAPFile on instance abapFile".
29080	Two extensions (TIBCO and Entity) are not triggered correctly in standard AIP installation vs using the flat.
29300	DMT remediation is not getting saved.
29400	Incorrect violation for the rule, "Avoid unsorted data after SELECT queries - 8134".
29499	All the Snapshots are getting deleted when "Stopping to Manage the Application" in CMS.
29614	Missing bookmark for rule, "Avoid Open SQL SELECT queries without WHERE condition on XXL Tables".
25692	Bookmarks for violations of the rule "Avoid Open SQL SELECT queries without WHERE condition on XXL Tables" (8464) are not displayed. This behaviour has now been changed and bookmarks are now available for violations raised by this rule.
29264	Incorrect sample and remediation sample are displayed in the rule "Avoid log forging vulnerabilities" (8044).
29315	User Input Security analysis shows no XSS rules in Engineering Dashboard.

### 8.3.34

## Feature Improvements

Summary	Details
User Input Security - @ModelAttribute annotation support	User Input Security is now able to detect violations for objects using the @ModelAttribute annotation from the SpringMVC framework. This improvement requires a recent release of the Security for Java extension (1.6.3-funcrel minimum): <a href="https://extend.castsoftware.com/#/extension?id=com.castsoftware.securityforjava&amp;version=latest">https://extend.castsoftware.com/#/extension?id=com.castsoftware.securityforjava&amp;version=latest</a> .
User Input Security - rule documentation improvement	The samples and remediation samples have been improved for the following quality rules: "Avoid HTTP response splitting - 7740" and "Avoid HTTP response splitting through API requests - 8484".

## Other Updates

Internal Id	Details
CAST-00000	The following legacy items are no longer provided in the AIP Core setup in the WARS folder: 1) CAST-CED.war and CAST-CED.ear (legacy CAST Engineering Dashboard/Discovery Portal), 2) CAST-AICP.war and CAST-AICP-admintools.zip (legacy CAST AIC Portal and related scripts). Note that CAST-CED.war and CAST-CED.ear are deprecated but still supported, therefore, if you require them, please contact CAST Support. CAST AIC Portal is no longer supported.
AIPCORE-3134	In previous releases of AIP Core, violations were erroneously being reported in the rule "Avoid use of a reversible one-way hash - 8416" instead of "Avoid weak cryptographic algorithm - 8414". This has now been corrected.

## Resolved Issues

Customer Ticket Id	Details
24420	Incorrect bookmark for the rule - "Avoid method invocation in a loop termination expression". The violation is a true violation, however bookmark is pointing to the whole method instead of the LOC that gets violated.
28837	Error - "null value in column rulelongdescription" is displayed when running an analysis.
22764	The Associated value is not generated for the QR: "Avoid using "nullable" Columns except in the last position in a Table".
28944	Mismatch in ADDED and TOTAL violations due to missing total scope, for the rule "Avoid file path manipulation vulnerabilities".
28987	DMT: the folders which are assigned to be ignored are not getting ignored. They are showing up in alerts even after re-packaging.
28132	False violation raised for rule: "Avoid using FOR ALL ENTRIES IN without emptiness check".
28759	After running the ABAP analysis, syntax errors were found for different files. ABAP analysis warning: ABAP.04: Unsupported syntax on DATA statement
28759	After running the ABAP analysis, syntax errors were found for different files. BAP analysis warning: ABAP.04: Unsupported syntax found at line: several statements
28764	Unsupported syntax (DATA --^ t_mkpj TYPE STANDARD TABLE OF ty_mkpj.) is found even when syntax is valid.
28766	Unsupported syntax "INTO @DATA(ls_vbak) UP TO 1 ROWS. -----^ ENDSELECT" found while syntax is valid.
28760	ABAP analysis warning: ABAP.04: Unsupported syntax found at line: CASE WHEN ( ( tvfk <sub>fkart_rl</sub> = 'LG' OR vbrk <sub>inv_type</sub> LIKE 'S%' OR vbrk <sub>inv_type</sub> = 'FAS' )
28768	Unsupported syntax: "UPDATE ('BSAD') SET xblnr = wk_xblnr "1913035 -----^ WHERE bukrs = wa_bseg-bukrs" found while syntax is valid.
28770	Unsupported syntax: "MODIFY zco_fc_cp FROM @( VALUE #( prctr = ip_ua -----^ pspnr = lv_pspnr )" found while syntax is valid
27609	Violation detected for the QR: 'Avoid Unreferenced Methods' for Lambda expressions.
27740	False Violation for the QR: "Avoid SQL queries that no index can support"
27788	The Exclusion rule: "Exclude the duplicate Dot Net project located inside the exactly same source folder" is not working and is creating AU for each project file.
27833	The remediation in the documentation does not provide example on how to validate the inputs.
28227	Links between Oracle Forms Triggers and Oracle Forms Procedures are missing.

28543	Reference finder is not creating the links as it removes the XML tag from the first line.
29128	Missing Link from Oracle Menu Item object and others like Oracle Forms Procedure.

### 8.3.33

#### Feature Improvements

Summary	Details
User Input Security - Support of analysis Execution Units/Groups	User Input Security analyses can now take advantage of Execution Unit grouping. This is primarily to improve analysis performance and to reduce the risk of an analysis crash.
User Input Security - improvements to the rule "Avoid HTTP response splitting - 7740" for both .NET and JEE	The User Input Security feature now has improved support for the rule "Avoid HTTP response splitting - 7740", for both .NET and JEE. Additional targets are now supported as follows: For NET: .NET, .NET Core, RestSharp. For JEE: javax.servlet, org.apache.cxf, org.apache.http, org.springframework.http, com.squareup.okhttp, okhttp3. As a result, analysis results may be impacted when re-analyzing existing unchanged source code - additional violations may be discovered.

#### Other Updates

Internal Id	Details
SAP-215	Refactoring of part of the SAP/ABAP analyzer has been implemented. This refactoring increases the maintainability of the analyzer while also increasing accuracy. As a result of the changes, some impacts to analysis results are to be expected when re-analyzing existing unchanged source code with this release: 1) Unresolved Objects are no longer created for SUBSTRING and CONCAT clauses. 2) Less violations will be returned for the rule "Avoid Artifacts with a Complex SELECT Clause - 7810" (the select clause column number was over-evaluated when "as <alias>" was present).
AIPCORE-2947	It is now possible to deliver Microsoft SQL Server .castextraction files (resulting from the CAST Database Extractor "Extract" option) via the new "Reuse existing CAST Extractor output" option for Microsoft SQL Server in the CAST Delivery Manager Tool.
AIPCORE-2948	It is now possible to deliver Sybase ASE .castextraction file (resulting from the CAST Database Extractor "Extract" option) via the new "Reuse existing CAST Extractor output" option for Sybase ASE in the CAST Delivery Manager Tool.

#### Resolved Issues

Customer Ticket Id	Details
27881	While upgrading schemas from 8.3.3 to 8.3.29, assessment model fails with an error message.
28277	Opening any saved view makes Enlighten crash.
28451	In CAST MS, DMT detects Java projects but analysis units (AUs) are not created post deployment.
28553	After upgrading to CSS4, python related errors are displayed in the analysis logs for the "extensions before" and "extensions after" steps.
28662	Snapshot is failing, at Create Architecture model, in Central schema step.
28555	Warnings are shown during analysis: "Internal error: Missing item in AST expression".

### 8.3.32

#### New Features

Summary	Details
---------	---------

Support for rules with 0 weight	This release introduces support for configuring rules with a weight of 0. When a rule is configured with a 0 weight, it is enabled (active) and will be triggered during an analysis, but it has no impact on any parent technical criterion, therefore it can be considered as a way to "preview" a rule without impacting the grade of the parent technical criteria and business criteria. In addition, rules with a 0 weight are never consolidated into the Measure schema, so will not appear in the Health Dashboard. See <a href="https://doc.castsoftware.com/display/AIPCORE/Grade+and+compliance+score+calculation">https://doc.castsoftware.com/display/AIPCORE/Grade+and+compliance+score+calculation</a> for more information.
---------------------------------	--

## Feature Improvements

Summary	Details
User Input Security - support for the .NET PostgreSQL framework	The User Input Security feature is now able to detect SQL injections for applications using the PostgreSQL (Npgsql) framework for .NET.
User Input Security - change of classification of some entry points	ASP.Net MVC and Struts2 entry points were tagged internally as "Network.input" in previous releases of AIP Core, however, these entry points are now classed as "Network.inputAPI". As a direct result of this change, violations found using these entry points will be classed as "violations through API". This change may impact analysis results when re-analyzing unchanged source code with this release of AIP Core: some rules will have less violations, others will have more.
User Input Security - support for the .NET RestWrapper framework	The User Input Security feature is now able to detect API injections for applications using the RestWrapper framework for .NET.
User Input Security - support for the .NET ServiceStack framework	The User Input Security feature is now able to detect API injections for applications using the ServiceStack framework for .NET.
User Input Security - support for the .NET RestSharp framework	The User Input Security feature is now able to detect API injections for applications using the RestSharp framework for .NET.
User Input Security - support for the .NET System.Net.Http.HttpClient framework	The User Input Security feature is now able to detect API injections for applications using System.Net.Http.HttpClient framework for .NET.
User Input Security - support for the .NET System.Net.WebClient framework	The User Input Security feature is now able to detect API injections for applications using System.Net.WebClient framework for .NET.
User Input Security - support for the .NET System.Net.WebRequest framework	The User Input Security feature is now able to detect API injections for applications using System.Net.WebRequest framework for .NET.

## Other Updates

Internal Id	Details
AIPCORE-3100	A recent update to McAfee's virus pattern has started to flag ExtensionDownloader.exe as malicious and is removing it from the installed location. ExtensionDownloader.exe has been updated in AIP Core 8.3.32 to resolve this issue.

## Resolved Issues

Customer Ticket Id	Details
23228	In the rules portal, search feature is not working for many quality rules and applications.
24358	Different formats for the same text is leading to different results in rules (For example: hard-coded and hardcoded).
24734	Tags are getting deleted from the static/tags.html interface, when the snapshots are deleted manually using CAST MS.

27582	Compute snapshot data is taking longer (running for 20+ hours instead of finishing in 10 hours).
27761	After the fix to remove empty analysis units was provided, it was observed that there were analysis units that had only WSDL files and no source files. Due to the missing source files the WSDL files were not analyzed hence there was a dip in SOAP operations.
27789	Procedure objects are not created from the "Reports files". Hence, info about Procedure objects is not found in the analysis results.
27792	While packaging the source in AIP 8.3.27, following fatal error message is displayed: Element type "message" must be followed by either attribute specifications, ">" or "/>".
27843	While performing task "Cleanup folder", intermittent fails (with an error) in step "Importing configuration".
27908	Maven AU config is not picking up the Java files in the folder "generated-entities"
27346	LOC value for the JEE technology shown by CAST AIP is more than expected after comparison with cloc tool. This fix will cause a decrease in LOC values for the JEE technology when analyzing unchanged source code with this release of AIP Core: in previous releases, LOC values for anonymous classes, inner classes and enums defined in classes were incorrectly counted twice. This change will also impact the results produced by the measure "Commented-out Code Lines/Code Lines ratio (% of LOC) - 7128".

## 8.3.31

### Feature Improvements

Summary	Details
User Input Security - improved support for .NET uncontrolled string format	User Input Security is now more precisely able to detect Uncontrolled string format vulnerabilities for .NET source code. As a consequence, some false positive violations reported when using previous releases of AIP Core may be removed.
User Input Security - improved support for the detection of SQL injections in applications using the Entity Framework for .NET	The methods SqlQuery and ExecuteSqlCommandAsync are now considered as database targets for SQL injection. System.Data.Find methods are no longer considered as database targets for SQL injection.
User Input Security - improved support for the detection of SQL injections in applications using the Oracle framework for .NET	The methods ExecuteNonQuery(), ExecuteReader(), ExecuteReader([System.Data] System.Data.CommandBehavior), ExecuteScalar() and ExecuteStream() are now considered as database targets for SQL injection.
User Input Security - improved support for the detection of SQL injections in applications using the Dapper framework for .NET	Methods such as QueryAsync, QueryFirstAsync, QueryFirstOrDefaultAsync etc. from the Dapper framework are now considered as database targets for SQL injection.
User Input Security - improved support for the detection of Log forging injections in applications using the logging framework System.Diagnostics.Trace for .NET	Methods such as TraceInformation, TraceWarning, TraceError etc. from the logging framework System.Diagnostics.Trace for .NET are now considered as database targets for Log forging injection.
User Input Security - support for the detection of deserialization injections in applications using the YAML framework for .NET	The methods Load([System.IO.TextReader) and Load([YamlDotNet.Core.IParser) from the YAML framework for .NET are now considered as targets for deserialization injection.
User Input Security - support for the detection of deserialization injections in applications using the XStream framework for JEE.	fromXML type methods from the XStream framework for JEE are now considered as targets for deserialization injection.

### Other Updates

Internal Id	Details
MAINFRA ME-520	The rule "Check PCB status code after DLI queries" ( <a href="https://technologies.castsoftware.com/rules?s=8160&amp;#124;qualityrules&amp;#124;8160">https://technologies.castsoftware.com/rules?s=8160&amp;#124;qualityrules&amp;#124;8160</a> ) has been modified to improve functionality. As a result of these changes your results may be impacted after upgrade.
MAINFRA ME-544	The rule "Variables defined in Working-Storage section must be initialized before to be read" ( <a href="https://technologies.castsoftware.com/rules?s=8034&amp;#124;qualityrules&amp;#124;8034">https://technologies.castsoftware.com/rules?s=8034&amp;#124;qualityrules&amp;#124;8034</a> ) has been modified to improve functionality. As a result of these changes your results may be impacted after upgrade.

### Resolved Issues

Customer Ticket Id	Details
--------------------	---------

22833	During analysis, links are missing between Oracle Forms Menu Item and Oracle Forms Module
25676	During Import Assessment Model, too many client msg and CMS are blocked
26062	During analysis, Java files are not analyzed (as the path is not covered in the AU though there is a reference in pom file)
27056	False Violation for the QR: Avoid SQL injection vulnerabilities
27169	During analysis, double links are created between two objects after UKB
27174	An improvement to the PB Analyzer has been implemented in this release of AIP Core: in order to produce more consistent analysis results, the behaviour of the .pbl data extraction process has been changed. Previously, source code was extracted from .pbl files only when it was considered necessary (i.e. no previous extraction had been completed for a given .pbl file, or when the .pbl file had changed since the last extraction). In this release of AIP Core, .pbl files will always be extracted to ensure that successive analysis results are consistent over time. As a result of this change, an error message will be recorded in the analysis log when extracted source code from a previous analysis is available, but the corresponding .pbl cannot be located in the new source code delivery. This indicates an issue with the organisation of your delivered source code which will need to be resolved. Example error message: "Error while retrieving information about a PB library, bad library name : path\to\my.pbl".
27267	During analysis, double links are created between two objects after UKB
27269	While adding a version in CAST-MS, error message is not displayed when the version name consists of * / (:)
27274	While adding a version in CAST-MS, error message is not displayed when the version name consists of * / (:)
27311	While running the update cast knowledge base (UKB) tool, following error is displayed: ERROR: relation "\$ctv_links" does not exist
27334	During snapshot, false violation for QR: "Avoid Uncontrolled format String"
27356	During snapshot, object name is truncated in Knowledge Base and Dashboard for COBOL Technology
27374	Analysis fails with the ERROR: relation "\$uax_import_instances" does not exist
27398	Application upgrade is failing in import package step with nullpointer exception
27554	Mainframe exclude copybook parameter is not active post upgrade (after migrating from 8.3.3 to 8.3.29)
26308	Missing links from JCL to Cobol Program when CALL syntax is used. This is now fixed and after an upgrade your existing results may be impacted.
27285	Mainframe Utilities (such as default utilities for zOS, AS400, IBM MQ etc.) are wrongly categorized as "Unknown Programs".
23758	3 Reference links out of 4 are invalid for QR "Call 'base.Dispose()' or 'MyBase.Finalize()' in the 'finally' block of 'Dispose(bool)' methods".

### 8.3.30

#### Feature Improvements

Summary	Details
Update AIP Core to allow custom CAST Storage Service /PostgreSQL L logins without SUPERUSER permission	AIP Core has been updated to allow logins to CAST Storage Service/PostgreSQL with custom PostgreSQL logins that do not have the SUPERUSER permission. Previously, custom logins required the SUPERUSER permission. See the following documentation: 1) <a href="https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+image+for+Docker#CASTStorageServicePostgreSQLImageforDocker-CASTAIP%E2%89%A58.3.12-customusers">https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+image+for+Docker#CASTStorageServicePostgreSQLImageforDocker-CASTAIP%E2%89%A58.3.12-customusers</a> , 2) <a href="https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++What+to+expect+after+installation#CASTStorageServiceWhattoexpectafterinstallation-Customdatabaseusers">https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++What+to+expect+after+installation#CASTStorageServiceWhattoexpectafterinstallation-Customdatabaseusers</a> , 3) <a href="https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+10+or+above+deployment+on+Linux#CASTStorageServicePostgreSQL10orabovedeploymentonLinux-CASTAIP%E2%89%A58.3.12-customusers">https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+10+or+above+deployment+on+Linux#CASTStorageServicePostgreSQL10orabovedeploymentonLinux-CASTAIP%E2%89%A58.3.12-customusers</a> and 4) <a href="https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+9.6.x+deployment+on+Linux#CASTStorageServicePostgreSQL9.6.xdeploymentonLinux-CASTAIP%E2%89%A58.3.12-customusers">https://doc.castsoftware.com/display/DOCCOM/CAST+Storage+Service++PostgreSQL+9.6.x+deployment+on+Linux#CASTStorageServicePostgreSQL9.6.xdeploymentonLinux-CASTAIP%E2%89%A58.3.12-customusers</a> .
Support for SAP PowerBuilder 2019	This release adds analysis support for SAP PowerBuilder 2019. No support of the new features introduced by this release. However applications built with this release and which are compliant with earlier releases of PowerBuilder, can be analyzed. There are no changes to the method of support, in other words, the PowerBuilder IDE is still required on the Analysis machine (see <a href="https://doc.castsoftware.com/display/TECHNOS/PowerBuilder++Required+third-party+software">https://doc.castsoftware.com/display/TECHNOS/PowerBuilder++Required+third-party+software</a> ).

Automatically discovered TF graph adjustment functions provided by Extensions or for bug-fixes	In addition to Standard and Custom adjustment functions, two new categories of adjustments are available in this release, both being enabled by default whether after a fresh AIP installation or after an upgrade: adjustments delivered by Extensions (future extension releases may take advantage of this new functionality) or adjustments delivered for bug-fixes. See <a href="https://doc.castsoftware.com/display/DOC83/TCC---+Using+Transaction+Graph+Adjustment">https://doc.castsoftware.com/display/DOC83/TCC---+Using+Transaction+Graph+Adjustment</a> for more information.
User Input Security - DynamoDB for .NET support	User Input Security is now able to detect NoSQL injections for applications using DynamoDB for .NET.
User Input Security - improved support for "org.springframework.jdbc" framework	User Input Security is now able to detect additional SQL injections for the org.springframework.jdbc framework.
User Input Security - support for "OWASP Java HTML Sanitizer" framework	User Input Security now supports the "OWASP Java HTML Sanitizer" framework as a valid sanitizer for the rule "Avoid reflected cross-site scripting".

## Other Updates

Internal Id	Details
AIPCORE-2703	Rules configured with 0 weight or with a 0 grade are no longer consolidated into the Measure schema, so will not appear in the Health Dashboard. Previously, rules with 0 weight were included in the grades of parent technical/business criteria provided in the Health Dashboard, therefore this change may impact your existing results if you had manually configured any rules with a 0 weight in the parent technical criteria.
MAINFRA ME-515	Violations located in "Unknown IMS Transaction" objects will no longer have a violation bookmark in the source code.
AIPCORE-2399	The User Input Security feature was incorrectly referencing the methods "Find" and "FindOneAndUpdate" (from the type MongoDB.Driver.IMongoCollectionExtensions) as possible violations for SQL injection instead flagging them as NoSQL injection violations. This bug has been fixed and this update may impact your existing analysis results.
AIPCORE-2839	An issue where end of line characters (Carriage Return Line Feed) were removed from the Sample and Remediation Sample sections in some Quality Rules when the text in the section is changed between releases of the extension or AIP Core, has been resolved. There is no impact to existing analysis results.

## Resolved Issues

Customer Ticket Id	Details
26772	A fix has been implemented to solve an issue where links from JCL Steps to SQL tables were not resolved due missing JCL SQL Query objects. This fix also requires SQL Analyzer 3.2.17. This issue has been fixed and this change may impact your analysis results on upgrading to 8.3.30.
26909	In previous releases, when the option "Save data and links to other data" was active, links between Cobol Paragraphs and Cobol File Links are not resolved. When the option is deactivated, the links are resolved. This mechanism has been reviewed and a new behaviour has been implemented: when the "Save data links to other data" is active, no link will be resolved between Cobol Paragraphs and Cobol File Links. Instead, a link will be resolved between the Cobol File Link and the Cobol Data variable.
26875	A fix has been implemented to solve an issue where links between Cobol Data and Cobol Data objects were not resolved. This issue has been fixed and this change may impact your analysis results on upgrading to 8.3.30.
26703	VB analysis fails with the error: SQL Error: ERROR: "Syntax error at or near 's'".

26777	There are wsdl files that have not been picked up by DMT which is causing issues in the SOAP operations objects not being identified by the analyzer.
26894	While running Appmarq Data Compiler, the process is aborted with an error message.
17423	The SQL Analyzer log contains many warnings of the type "GUID duplicate found".
23238	Performance issue in the CAST Transaction Configuration Center Enhancement view because of duplicate transaction links for Struts objects

## 8.3.29

### Feature Improvements

Summary	Details
User Input Security - entry-points	The method <code>javax.servlet.HttpServletRequest.getInputStream</code> is now considered as an entry-point for the User Input Security. This change may impact your analysis results on upgrading to 8.3.29.
User Input Security - Avoid weak cryptographic algorithm - 8414	The following cryptographic algorithms are now considered as dangerous for the quality rule "Avoid weak cryptographic algorithm - 8414": RC2 and PBEWithMD5AndDES. This change may impact your analysis results on upgrading to 8.3.29.
User Input Security - MainCounterValue parameter	User Input Security: The default <code>MainCounterValue</code> parameter has been changed from 15000 to 1000. This parameter governs the number of steps that are searched to find flaws. This change has been introduced to provide a value that is more suited to the vast majority of analyzed Applications. Reducing the default value to 1000 will provide a significant performance improvement (reduced analysis duration) while not adversely impacting the number of flaws that are found (a negligible number of flaws may not be found using the new parameter value). CAST recommends restoring the original value of 15000 if your analysis runtime was satisfactory - this will ensure that you get the same behaviour and results as in previous releases of AIP. If your analysis runtime with the previous default value was very long, test the new value in a new analysis to ensure that the number of flaws returned is not adversely affected.
User Input Security - new rule Avoid deserialization injection - 8524	A new rule has been implemented for both JEE and .NET technologies called "Avoid deserialization injection - 8524". The following frameworks are supported: JEE - <code>java.io.ObjectInputStream</code> , <code>com.esotericsoftware.kryo.Kryo</code> and <code>java.beans.XMLDecoder</code> . .NET - <code>System.Xml.Serialization.XmlSerializer</code> . Your existing analysis results may be impacted by the addition of this new rule.
User Input Security - Avoid resource injection - 8442	The rule "Avoid resource injection - 8442" has been updated to take into account violations of type "Avoid Connection String Parameter Pollution", for both JEE and .NET technologies. This change may impact your analysis results on upgrading to 8.3.29.
User Input Security - Avoid log forging vulnerabilities - 8044	Methods such as "logError" or "logWarning" are now recognized and are automatically assigned as targets for the quality rule "Avoid log forging vulnerabilities - 8044". This change may impact your analysis results on upgrading to 8.3.29.

### Other Updates

Internal Id	Details
AIPCORE-2504	Update to fix an "out of memory" exception when using the "Open dashboard" option in CAST Management Studio. The JVM used to launch the dashboard is now opened with the options <code>Xms1024m -Xmx2048m</code> . Previously <code>-Xms128m</code> and <code>-Xmx512m</code> were used.
AIPCORE-2565	.NET Framework 4.7.2 is now installed (if it is not already present on the target server) by the AIP Core 8.3.29 setup for new installations. If a more recent release of the .NET Framework is present on the target server already, .NET Framework 4.7.2 will not be installed. When upgrading to AIP Core 8.3.29 from a previous release, .NET Framework 4.7.2 will not be installed.

AIPCORE-2574	Cosmetic update to the formula used to calculate the Effort Complexity (EC) Total value in the CAST Transaction Configuration Center. The formula displayed in the report and in the CAST Transaction Configuration Center was wrongly showing that EC Deleted values were used to calculate the EC Total value. The formula used by the CAST Transaction Configuration Center is correct, therefore there are no impacts to existing analysis results.
AIPCORE-2511	User Input Security - URLs in the following rules have been updated as they were previously giving 404 responses: "Avoid log forging vulnerabilities - 8044", "Avoid using insufficient random values for cookie - 8242" and "Avoid log forging vulnerabilities through API requests - 8508"
AIPCORE-2369	User Input Security - A remediation sample has been added for the rule "Avoid mixing trusted and untrusted data in HTTP requests - 8238" which was previously missing.
AIPCORE-1994	User Input Security - The description provided in the rule documentation for "Avoid using unsecured cookie - 8240" has been updated to clarify that the rule only considers cookie secured in the source code, and not the cookies that are secured globally using the config file.
AIPCORE-2607	User Input Security - The documentation of the rules "Avoid weak cryptographic algorithm - 8414" and "Avoid use of a reversible one-way hash - 8416" has been updated to provide greater accuracy.
AIPCORE-2624	User Input Security - multiple updates to rule descriptions: the sentence "List all methods that miss calling the required input validation calls" has been changed to "List all methods that make resource calls forged by user input" wherever it occurs.
AIPCORE-2540	User Input Security - the property System.Web.HttpRequest.PhysicalApplicationPath was previously incorrectly assigned as a user input. This issue has now been fixed. This change may impact your analysis results on upgrading to 8.3.29.
AIPCORE-2372	User Input Security - previously some methods were incorrectly tagged as targets for the rule the rule "Avoid file path manipulation vulnerabilities - 7752" causing false violations. This issue has been fixed. This change may impact your analysis results on upgrading to 8.3.29.

## Resolved Issues

Customer Ticket Id	Details
18364	False positive for QR "Avoid Programs with lines of more than 80 characters"
18485	False positive for the rule Avoid 'Select *' statement
21798	False positive for "Avoid unreferenced Classes", due to FacesConverter annotation. Note: This rule has been removed for JEE in 8.3.29.
21825	False positive for- Avoid unreferenced classes when methods of that class are called. Note: This rule has been removed for JEE in 8.3.29.
22512	Error VB6 analyzer "Inference Engine has returned an unexpected error"
22600	Description update for the rule id 8240 : 'Avoid using unsecured cookie'
23171	CMS part - Snapshot is stuck due to a blocked query
23323	Warnings in MA SQL extension analysis: [MAv2] Cannot find type of string or comment
24486	False violation: Avoid file path manipulation vulnerabilities
24850	Include remediation sample for the rule "Avoid mixing trusted and untrusted data in HTTP requests"
25115	PowerBuilder analysis warnings: the UTF-8 sequence starting at offset 0 was invalid
25366	False positive - Using SEARCH ALL only with sorted data
25367	The Rule "Avoid unchecked return code (SQLCODE) after EXEC SQL query" has False positive violations shown in the AED
25463	CAST AIP Upgrade Automation script is failing when there are spaces in the folders configured in CASTUpgrade_Config.txt
25693	Upgrade 8.3.16 > 8.3.26 is failing with error : Inconsistency found in metamodel
25701	Error during migration from CAST AIP 8.2.7 to 8.3.26 - "Invalid Field delivery.SourceFilesPackage.lastExtractionDate "
25748	In technical index under Avoid log forging vulnerabilities - invalid OWASP reference URL
25866	False positive violations in the rule 'Never truncate data in MOVE statements'
25906	False violation "Never truncate data in MOVE statements"
25939	C/C++ files did not get analyzed with C and C++ File discoverer
26072	False violation "Never truncate data in MOVE statements"
26098	Effort Complexity (EC) Computation is off by 1

26196	Empty DMT projects are not exported to CAST-MS, resulting in associated Analysis Units being deleted and an adverse impact on analysis results. Some of these Analysis Units should not be deleted since they may have been configured manually.
26400	Problem - Set as current version fails - _connection Error Set standard_conforming_strings=on
26540	Snapshot fails with error: Source Server/BCD(LCB Quotes) full content.Module name: Unexpected character (.

## 8.3.28

### Feature Improvements

Summary	Details
Metrics Assistant - all technologies	When the following issues are encountered during the processing of the Metrics Assistant an error is displayed, stopping the analysis: "An ill-formed token has been encountered during scanning..." and "[MAv2] Error in function Accept...". These issues are now considered as warnings rather than errors, to prevent the analysis process from stopping.

## 8.3.27

### Feature Improvements

Summary	Details
CAST Storage Service backup and restore tools	A change has been made to the CSSBackup.exe and CSSBackupAll.exe tools provided with CAST AIP to provide compatibility with current CAST PG releases. As such, schema backups created with CSSBackup/CSSBackupAll included in 8.3.27 (and any higher 8.3 service pack) should only be restored with CSSRestore/CSSRestoreAll included in 8.3.27 (and any higher 8.3 service pack).

### Other Updates

Internal Id	Details
AIPCORE-2364	The URL used to connect to CAST Extend has been changed by default to <a href="https://extend.castsoftware.com">https://extend.castsoftware.com</a> .
AIPCORE-2420	The automatic blackboxing action will now identify as database targets all methods beginning with (previously only Find or find were considered as targets): Find(), FindRow(), FindRows(), FindColumn(), FindColumns().
AIPCORE-2194	Support (predefined methods) has been added for the GWT (Google Web Kit) framework.
AIPCORE-2395	Sanitization methods for the NpgSql framework for JEE are now supported.
AIPCORE-2341	The rule "8518 - Avoid regular expression injection" has been implemented for JEE technologies. Previously this rule only functioned on .NET technologies.

### Resolved Issues

Customer Ticket Id	Details
23232	Missing links from "Java Method" to "Stored Procedure Objects", whenever there is a call with full procedure name.
23446	Few QRs are missing from the Dashboard (as these QRs are not configured to take Java technology into account).
24293	Central base is shown in a wrong triplet in Server Manager (though removed from the older system).
24356	SQL Query objects are deleted in TFP and Transaction call graph is marked as modified.
24673	Analysis units are not created when the source code consists website.publishproj, and due to this .aspx files are not analysed.
24747	For any application name containing "&" (special character), the logs were blank when checked in CMS.

24841	Internal exceptions were recorded in the analysis log when the analyzer attempts to parse a .MFS file.
24891	ED dashboard not showing deleted violations.
24971	Objects created from IMS DB files have data function names that have the object name enclosed in parantheses.
25135	Source code is not displayed in Engineering Dashboard for the rule: "avoid direct or indirect remote calls inside a loop".
25174	Fatal error on Merging step:duplicate key value violates unique constraint "pk_objdsc".
25434	Unable to launch DMT from AIC Portal - org.apache.commons.io.IOUtils.readFully(Ljava/io/InputStream;[B)V.
25370	An error message is displayed in the CAST Transaction Configuration Center log stating that the Base_Mainframe.TCCSetup delivered in AIP 8.3.26 is syntactically incorrect: Message ERR: Could not load Configuration from file \configuration\TCC\Base_Mainframe.TCCSetup Message ERR: Exception: com.castsoftware.java.InternalException: Data Set definition file XML parsing returned errors.

## 8.3.26

### Feature Improvements

Summary	Details
Mainframe Analyzer as an extension	The Mainframe Analyzer has been externalised as an extension to give the feature more flexibility to future development. The Mainframe Analyzer embedded in AIP Core will continue to exist and will be shipped "out of the box" with AIP Core. Critical bugs will continue to be fixed on the Mainframe Analyzer embedded in AIP Core but no new features or functionality will be added. The new Mainframe Analyzer extension will have exactly the same features and functionality on release as the Mainframe Analyzer embedded in AIP Core, therefore analysis results will be identical. The new Mainframe Analyzer is compatible with AIP Core 8.3.26. All future development of the Mainframe Analyzer (new features, functionality etc.) will be completed in the Mainframe Analyzer extension only. Critical bug fixes will be fixed in the Mainframe Analyzer extension (as well as the analyzer embedded in AIP Core). The behaviour is as follows: Nothing is automatic - for both AIP Console and "legacy" CAST AIP deployments, the Mainframe Analyzer extension must be manually downloaded and installed in order to use it. If the extension is installed, CAST AIP Console/CAST Management Studio will automatically detect that it exists and will use the extension rather than the analyzer embedded in AIP Core. Once the extension has been installed and used to produce analysis results, it is not possible to reverse this choice by removing the extension and re-analyzing the source code again.
Updates to Base_Mainframe.TCCSetup for transaction configuration	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.
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.
User Input Security	User Input Security now supports the framework Microsoft.Practices.EnterpriseLibrary, including the sanitization of this framework.
User Input Security	User Input Security now supports the framework apache-httpcomponents-httpclient, including the sanitization of this framework. Note that this framework was previously supported through a User Community extension: <a href="https://github.com/CAST-Extend/com.castsoftware.uc.apache.httpclient.blackboxes">https://github.com/CAST-Extend/com.castsoftware.uc.apache.httpclient.blackboxes</a> - this extension is no longer required if you are using AIP 8.3.26.
User Input Security	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.
New User Input Security related rule	8518 Regular expression injection. Input name = "Network.read". Target name = "Regexp.write". Partial .NET support. No support for JEE.

New User Input Security related rule	8520 Regular expression injection (second order). Input name = "Network.readDatabase". Target name = "Regexp.write". Partial .NET support. No support for JEE.
New User Input Security related rule	8522 Regular expression injection through API. Input name = "Network.readAPI". Target name = "Regexp.write". Partial .NET support. No support for JEE.
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 follows: 0.8=1, 0.5=1, 0.2=1, 1.8=2, 1.5=2, 1.2=2. These results can be seen in the "TCC - Enhancement node - Right hand panel".

## Resolved Issues

Customer Ticket Id	Details
20225	When set as current version, analysis unit is being created for a CPP Project file even with missing Source files.
23612	AIP Console displays deactivated analysis units for .NET core apps.
23717	False violations are displayed 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.
23981	Analysis is failing even when the DLM rule file is not present in CMS.
24122	Generation of SRD files in PowerBuilder analysis is not consistent
24252	Incorrect detection of Hibernate version in DMT. When Java source is packaged in DMT, the Hibernate version detected is not correct, which led to missing links in analysis result.
24423	Many fatal errors are displayed in the logs that are not actually fatal.
24481	AETP is displayed as 0, though there are added/removed/updated technical objects.
24531	False violations are displayed.
24572	JCL Batch transactions are not correctly created by the analyzer.
24578	For some objects, the Mainframe analyzer has used the OBJECT_FULL_NAME value for the OBJECT_NAME in the CDT_OBJECTS table. The OBJECT_NAME value should be different to OBJECT_FULL_NAME.
24642	False violations are displayed for the rule "Never truncate data in MOVE statements - 7688".

## 8.3.25

### Note

CSS Upgrade Wizard (used to move schemas from one CAST Storage Service/PostgreSQL instance to another) is now deprecated and is replaced by the CombinedTransfer.bat file - see below. CAST AIC Portal is now deprecated and official support for this web application will cease at the end of 2020. CAST encourages users to switch to AIP Console where possible (<https://doc.castsoftware.com/display/AIPCONSOLE> /[/Import+an+Application+managed+with+CAST+Management+Studio+into+AIP+Console](https://doc.castsoftware.com/display/AIPCONSOLE)).

## Feature Improvements

Summary	Details
Mainframe Analyzer - Support for IMS MFS Maps	Support has been implemented for IMS MFS Maps to improve IMS/DC support so that it is possible to find out which Cobol programs use an MFS Map: MFS Maps are contained in files with the extension *.mfs. FMT macro defines the map (called "format" in IMS vocabulary). MSG macro defines MID and MOD messages. MID are those that have the INPUT type and MOD are those that have the OUTPUT type. MID and MOD identifiers are specified in the IO-PCB. In the MID/MOD structure, there is a field that contains the name of the transaction. This information allows the analyzer to create links between MFS Maps and transactions. As a result, some changes have been implemented: The Mainframe Discoverer ( <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe+Discoverer">https://doc.castsoftware.com/display/TECHNOS/Mainframe+Discoverer</a> ) will detect a project (and therefore automatically create an Analysis Unit) for each *.mfs file discovered in a folder. .mfs files have been added to the list of files that will be automatically analyzed - see for example <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+configuration">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+configuration</a> . New object types will be resolved for IMS Message Format Service, IMS Message Input Descriptor and IMS Message Output Descriptor - see <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+results">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+results</a> .

Mainframe Analyzer - Improved support for JCL Dataset sub types	The Mainframe Analyzer is now able to detect the following specific types of JCL Dataset, which will now be visible in CAST Enlighten, Architecture Checker and CAST Transaction Configuration. See <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Technical+notes#MainframeTechnicalnotes-dataset">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Technical+notes#MainframeTechnicalnotes-dataset</a> for more details: GDG datasets, PDS datasets, DBD datasets, GSAM datasets, VSAM datasets, Temporary datasets. In addition, a new prototype link has been implemented between DBD objects and JCL Datasets (DBD).
Rule documentation update	The "Rationale" section for the Mainframe related rule "8468 - Program semantic should respect the logic of flow execution" has been updated.
SQL Analyzer embedded in AIP	The SQL Analyzer embedded in AIP now supports (by reference) the analysis of databases hosted on: Microsoft SQL Server 2016, 2017 and 2019, however no new syntax or features introduced in these newer releases are supported. Sybase ASE 16, however no new syntax or features introduced in this newer release are supported.
User Input Security - new rules	The following rules have been implemented in this release, targeting the JEE technology: 8482 - 8516 (see <a href="https://technologies.castsoftware.com/rules?sec=srs_aip&amp;ref=#124;8.3.25_2403">https://technologies.castsoftware.com/rules?sec=srs_aip&amp;ref=#124;8.3.25_2403</a> ). All of the above new rules are based on "injection through API requests" - the list of supported APIs is as follows: javax.ws.rs-api-2.1, jersey-client-1.19.4, resteasy-client, cxf-rt-frontend-jaxrs-2.7.18, wink-client-1.4, resthub-web-client-2.2.0.
User Input Security - Improvement to support for Apache Struts 2 applications	The following truncated manglings are now supported: com.opensymphony.xwork2.DefaultTextProvider.getText, com.opensymphony.xwork2.ActionSupport.getText, com.opensymphony.xwork2.validator.DelegatingValidatorContext.getText, com.opensymphony.xwork2.CompositeTextProvider.getText, com.opensymphony.xwork2.TextProviderSupport.getText, com.opensymphony.xwork2.TextProvider.getText. This is an improvement to "AIPCORE-1705 - User Input Security is now able to detect security violations in Apache Struts 2 applications" added in AIP Core 8.3.21.
CAST Database Extractor	The CAST Database Extractor now support (by reference) the extraction of databases hosted on: Microsoft SQL Server 2016, 2017 and 2019, however the extractor will handle the databases as Microsoft SQL Server 2014 databases and no new syntax or features introduced in these newer releases are supported. Sybase ASE 16, however the extractor will handle the databases as Sybase ASE 15.x databases and no new syntax or features introduced in this newer release are supported.
CombinedTransfer.bat	A new batch file called CombinedTransfer.bat has been created as a replacement for the CSS Upgrade Wizard (now deprecated). It is a wrapper batch file for the CSS Backup and Restore Tools ( <a href="https://doc.castsoftware.com/display/STORAGE/Maintenance+activities+for+CAST+Storage+Service+and+PostgreSQL">https://doc.castsoftware.com/display/STORAGE/Maintenance+activities+for+CAST+Storage+Service+and+PostgreSQL</a> ), provided as part of the AIP Core 8.3.x, and involves a fully automated process of dumping the required schemas to file and then restoring the dumps on the new server. The CAST Storage Services /PostgreSQL do not need to be installed on the same host, and both can be remote to the machine on which you are executing the batch file. The CombinedTransfer.bat batch file is located in the following folder and must be executed from within the context of this folder: <CAST AIP installation>\CSSAdmin\CSSUpgrade\ See <a href="https://doc.castsoftware.com/display/STORAGE/Moving+existing+schemas+to+a+new+CAST+Storage+Service+or+PostgreSQL+instance">https://doc.castsoftware.com/display/STORAGE/Moving+existing+schemas+to+a+new+CAST+Storage+Service+or+PostgreSQL+instance</a> for more information.

## Other Updates

Internal Id	Details
CAST-00000	CAST Management Studio - Create application option: If you need to onboard new Applications and are not yet using AIP Console or are having issues using CAST AIC Portal, then it is now possible to create new Applications directly in CAST Management Studio for all user audiences ("regular" through to "expert"). This is a "stop gap" solution until such time as you are ready to switch to AIP Console ( <a href="https://doc.castsoftware.com/display/AIPCONSOLE/Import+an+Application+managed+with+CAST+Management+Studio+into+AIP+Console">https://doc.castsoftware.com/display/AIPCONSOLE/Import+an+Application+managed+with+CAST+Management+Studio+into+AIP+Console</a> ).

## Resolved Issues

Customer Ticket Id	Details
22135	While performing Oracle 12c r2 database extraction, using DMT from AIP 8.3.20, an error is displayed.
22978	CSV task takes too long (3 days).
23059	In the POM project, the source code files defined under build-helper-maven-plugin are not picked by DMT under the POM project.
23309	The Mainframe analysis crashes with the following error: "The analysis has not ended correctly (Error code -1073741819)."
23386	The analysis is stuck processing one specific .ABAP file when the "Number of Instances" value is set to 200000 in CAST Management Studio - changing this to 400000 allows the analysis to complete.
23454	While analyzing, the Universal Importer (UI) is taking uax files in the tmp folder into account.
23529	When unregistering a CB/KB from the MNGT, the corresponding sync tables are not getting updated.

23530	Unable to edit or select the deprecated attribute in General tab, while creating a custom rule in CMS.
23646	While running the packaging for a .castextraction file, the extraction completes without any error, though there is no .castextraction file present in the location.

## 8.3.24

### Feature Improvements

Summary	Details
Mainframe Analyzer - Improved VSAM file support	upport introduced for VSAM commands in "SYSIN" clauses, for example: ALLOCATE, ALTER, DEFINE, DELETE, EXAMINE, LISTALC, LISTCAT, LISTDS, PRINT, REPRO, VERIFY. Support introduced for If IDCAMS utility and VSAM data-set types (for Cobol and JCL) when they call indexed, relative and sequential organisation: Entry-sequenced data set (ESDS), Key-sequenced data set (KSDS), Relative-record data set (RRDS).
Mainframe - new rules implemented	The following new rules have been implemented: 8468, 8470, 8476, 8478, 8780. See <a href="https://technologies.castsoftware.com/rules?sec=srs_aip&amp;ref=#124;#124;8.3.24_2371">https://technologies.castsoftware.com/rules?sec=srs_aip&amp;ref=#124;#124;8.3.24_2371</a> .
SSL connection to CAST Storage Service /PostgreSQL	CAST AIP 8.3.24 introduces support for connecting to CAST Storage Service/PostgreSQL instances using an SSL encrypted connection. Support for encrypted SSL connections requires some configuration for both the CAST Storage Service/PostgreSQL instances and CAST AIP itself. See <a href="https://doc.castsoftware.com/display/STORAGE/SSL+encrypted+mode+configuration+for+CAST+Storage+Service+and+PostgreSQL">https://doc.castsoftware.com/display/STORAGE/SSL+encrypted+mode+configuration+for+CAST+Storage+Service+and+PostgreSQL</a> .
User Input Security - rule documentation	The following changes have been applied to the documentation (no impact on analysis results) for the rule "8438 Avoid code injection": The Reference section has been updated to change the CWE reference from 78 to 94 and 95.
Miscellaneous - long path support	When using CAST AIP, the path of some log files and other internal files may exceed the total number of characters permitted for a path in Microsoft Windows (260 characters by default). This is especially true when enabling the User Input Security feature for .NET and JEE technologies. When a path exceeds 260 characters, the analysis (or feature) would usually crash, for example the User Input Security would crash with the errors "System.IO.PathTooLongException" or "System.InvalidOperationException". To avoid crashes due to situations where the long path limitation is exceeded, two changes need to be made: Enable long path support in Microsoft Windows (Windows 10/Windows Server 2016 or above only) - see <a href="https://docs.microsoft.com/en-us/windows/win32/fileio/naming-a-file#enable-long-paths-in-windows-10-version-1607-and-later">https://docs.microsoft.com/en-us/windows/win32/fileio/naming-a-file#enable-long-paths-in-windows-10-version-1607-and-later</a> for more information. Use AIP Core 8.3.13 and, where appropriate: JEE Analyzer extension 1.0.21 and Security for Java extension 1.4.5.
Miscellaneous - Change to SET_DEFINITIONS table	The table SET_DEFINITIONS (Analysis schema) has been modified: the column "setprocedure" will now accept a procedure name up to 255 characters in CAST AIP 8.3.24. Previously this column only accepted procedure names with a maximum of 30 characters. Note that if extensions are to be compatible with older releases of CAST AIP, they must still use 30 characters max.

### Resolved Issues

Customer Ticket Id	Details
22712	While viewing the rule documentation for "Avoid having multiple artifacts deleting data on the same SQL table" (7392), the Remediation code and the Sample source code is not correct. (Description of the rule needs to be updated).
22938	While launching snapshot in CMS GUI fails with an error, when the previous snapshot was killed at "Compute snapshot" step.
22978	CSV task takes too long (3 days).
23036	AAD consolidation takes longer when CLI/GUI is used. (Issue is due to the fact that there will be more number of rows in dss_date_snapshot than dss_snapshots. Both tables are expected to contain same number of rows).
23129	While migrating (to the 8.3.22 version from 8.3.14) using batch file upgrade process - in the Delivery folder, if "sources.CastSourcePackage" is deleted manually, then when the batch file upgrade is run, the automatic delivery step allows the set current version step to succeed (but it is expected to fail).
23324	Wrong results for analyzers, using environment profiles (mainly Java and C++).

## 8.3.23

### Note

Starting from this release of AIP Core, CAST Architecture Checker will no longer be installed as part of the AIP Core setup, whether installing from scratch or on a server where a previous release exists. CAST Architecture Checker has evolved into a standalone component where all feature requests and bug fixes are now managed. This standalone component can be downloaded from CAST Extend (<https://extendng.castsoftware.com/#/search-results?q=archichecker>). Note that the AIP Core setup will create a Windows Start menu shortcut for CAST Architecture Checker - when clicked, a popup message is displayed explaining that CAST Architecture Checker can be downloaded from CAST Extend.

### Feature Improvements

Summary	Details
CAST Delivery Manager Tool - Auto selection of Maven JAR files	In CAST AIP 8.3.23, if a JAR named after the name of the requested artifact is provided in the source code folder, it is accepted and a missing artifact alert is no longer raised. Previously, a manual remediation task was required to associate a JAR to a missing Maven project. Now, it is automatic. As a result of this change, for Maven projects, there may be no need to provide a Maven resource package if the corresponding JAR files have been provided in a sub-folder of the source package. Note that this behaviour does not apply to Gradle based projects. Any required Maven repositories must be delivered manually.
CAST Delivery Manager Tool - Change to the selection of artifacts with non-standard qualifiers in the version name	In CAST AIP 8.3.23, the CAST Delivery Manager Tool will remove non-standard qualifiers before comparing the Maven versions, so that, even if the plain version is lower than the qualified version, it can be accepted as a suitable version.
User Input Security - Change to support of org.springframework.jdbc	In previous releases of CAST AIP, support of the API org.springframework.jdbc for the User Input Security feature relied on automatic blackboxing. In CAST AIP 8.3.23, this has now changed and static rules will be used instead. Note that this change may impact existing analysis results.
User Input Security - Error handling improvement	If the User Input Security has no file(s) to analyze this is highly likely to be due to an internal bug. In this situation, the User Input Security will now report an error instead of indicating that the analysis has succeeded.
User Input Security - Variations in the number of violations between two consecutive snapshots with the same source code	A bug has been fixed which was causing varying numbers of violations to be displayed for certain User Input Security related rules between two consecutive snapshots of the same application with unchanged source code. This was due to a bug causing different paths to be calculated for a given endpoint.
User Input Security - Documentation updates	A new page has been added to help users improve the performance of an analysis that includes a User Input Security check. See <a href="https://doc.castsoftware.com/display/DOC83/User+Input+Security+-+Advanced+configuration+to+improve+performance">https://doc.castsoftware.com/display/DOC83/User+Input+Security+-+Advanced+configuration+to+improve+performance</a> for more information.
User Input Security - SecurityAnalyzer.log updates	A minor change has been made to change a message level from WARN to INFO: "Reached new field resolution algorithm failure count limit (10), will use default field resolution algorithm, next time."

User Input Security - Rule documentation updates	The Sample section of the rule "8098 Avoid uncontrolled format string" has been updated since it contained an error. The Description section of the rule "8240 Avoid using unsecured cookie" has been updated to include a limitation: "Limitation: in .NET environments, this rule does not check if the key requireSSL in web.config file."
CAST Transaction Configuration Center - Change in behaviour when loading .TCCSetup configuration files (the automatic configuration refresh process)	Previously when uploading a .TCCSetup file which already existed and where the package-version of the file differs with the existing package-version in the Management schema, the following behaviour was used: each rule will be loaded with status active by default, except if the rule was present in the previous version, its definition is unchanged, and it had been manually deactivated by the user, in that case, the rule will be set to inactive as well. From CAST AIP 8.3.23, this behaviour changes as follows (see also <a href="https://doc.castsoftware.com/pages/viewpage.action?pageId=264224227">https://doc.castsoftware.com/pages/viewpage.action?pageId=264224227</a> ): Each rule which was present in the previous version will be loaded with the same status as before, whichever the definition of this rule is the same or has changed. In this latter case, a warning will be logged to inform the user of this change, as in the example below where both the definition of an active Entry Point rule and of a deactivated End Point rule have both changed in a new version of the 'Base_HTML5' package: WRN: -the rule "Standard Entry Point - HTML5 AspDotNet" (type=Transaction entry points) will remain active because although its definition has changed, it has the same name and type as the previously active rule "Standard Entry Point - HTML5 AspDotNet" (type=Transaction entry points). WRN: -the rule "Standard End Point - HTML5" (type=Transaction end points) will remain deactivated because although its definition has changed, it has the same name and type as the previously deactivated rule "Standard End Point - HTML5 (type=Transaction end points)".

## Resolved Issues

Customer Ticket Id	Details
19880	An error is displayed while saving an object (with external parent).
20407	2586: Utilization of "DoEvents" inside a loop": rule description is not insufficient (it needs to be more descriptive). After review, this rule has now been disabled in 8.3.23 out of the box.
22119	CAST AIP 8.3.20 installation runs for long time, it neither gets completed nor throws any error.
22414	When a qualifier is present in the version name POM is not picked up from the Maven repository (jar files were not picked by DMT).
22504	DMT fails to identify presence of JAR dependencies, unless provided in Maven format. When the JAR/WAR files corresponding to Maven artifacts are provided directly in the sources, they are not recognized by the DMT, and alerts are raised.
22688	Warning message (which does not have any impact) is displayed during analysis of security log file.
22771	Snapshot is taking long time during the execution of procedure - DIAG_SCOPE_JEEAMDA003.

## 8.3.22

### Feature Improvements

Summary	Details
Mainframe Analyzer Support for links from JCL to Java	Support has been introduced for situations where JCL batches are executing Java (a new Mainframe object has been added for this situation):.
Mainframe Analyzer - Support for links from JCL to SQL	The following methods that can be used to process SQL/access database within JCL are now supported: INZUTILB utility DSNTIAUL utility Control Card file (.ctr) A new Mainframe object has been added for this situation.
Mainframe Analyzer - JCL Symbol resolution	JCL symbolic parameter values are now correctly propagated from JCL to procedures in the call chain.
User Input Security	User Input Security is now able to detect security violations in Spring JDBC framework applications.

Architecture Models	Architecture Models attached to an application are now saved in the Dashboard schema during the snapshot computation, this is so that the graphical representation of the model can be reproduced in the CAST Engineering Dashboard along with the results of the associated rules (metrics). This is in preparation for a future release of the CAST Engineering Dashboard where this feature will be implemented.
Extension installation - more stringent checks applied	When an extension is installed (on its own, as part of a schema installation or as part of a schema upgrade), more stringent consistency checks are now run on the metamodel XML file included in the extension: for all numeric fields: when starting with "0", a number is now considered as decimal and no longer as octal. For the file_no field the value should be between 0 and (INT_MAX / 1000) - 1 = 214748. These checks should not cause any issues with the installation of official CAST AIP extensions however, if you are using custom extensions that do not conform to the metamodel syntax, the extension installation process may fail (schema installation/schema upgrade may also fail).

## Resolved Issues

Customer Ticket Id	Details
19498	DMT Packaging alerts will differ depending on whether a sub-folder (in the root path) is specified in the "Folders to extract" option. Source code extracted is identical.
20783	While delivering V2 through a Delivery Manager Tool automation script. .NET framework assemblies files are getting removed automatically and no project is identified in V2.
21123	Analysis is stopped, as Console fails to filter non-manageable extensions. This results in the error "Update Extensions failed".
21174	When installing/upgrading a custom extension that contains syntactical errors, for example if the first line in the metamodel xml file contains "0" as the first digit. E.g.: <metaModel file_level="client" file_no="073">. The installation/upgrade of the extension fails.
21889	When looking at the number of violations for a given rule in the Risk Investigation view in the Engineering Dashboard - the number of violations displayed in the left hand panel differs to the number of violations displayed in the right hand panel.
22031	Error is displayed during the validation step of DMT packaging.
22064	When using the Action Plan Optimizer and selecting an Application the scroll bar is missing therefore when there are many Applications some cannot be selected since they are hidden.
22065	When looking at the results of the rule Never truncate data in MOVE statements - 7688, false violations were being reported where only one variable of OCCURS ... DEPENDING ON exists.
22109	Snapshot generation is taking longer in compute snapshot step.
22123	When looking at the results of the rule Avoid Packages with High Afferent Coupling (CA) - 7248: inconsistency in the number of reported violations.
22246	While searching the rule, "never truncate data in move statement" in ED Dashboard: incorrect bookmarks displayed for violations.

## 8.3.21

### Feature Improvements

Summary	Details
Upgrade - delivery folder consistency check has been implemented	During an upgrade to CAST AIP 8.3.21, a consistency check has been implemented to ensure that the index.xml file located in the folder Delivery\plugins and the plugins (i.e. sub-folders) present in the Delivery\plugins folder are consistent. This check has been added to avoid situations where, for example, the version of a plugin (e.g. discoverer or an extractor) located in the Delivery\plugins folder and the reference to that plugin version in the index.xml file, differ. If any inconsistencies are detected during the upgrade, these will be logged in a new log file called ServMan-Utils produced by CAST Server Manager, located here (if the default settings are used): %PROGRAMDATA%\CAST\CAST\Logs\ServMan\. Where possible, inconsistencies are repaired. When this is not possible, the upgrade stops with and an error is logged in the main CAST Server Manager log file, located in the same folder as above.
Mainframe Analyzer - IBM MQSeries updates	Syntax coverage has been improved when using data from JCL. The following is now supported: FROM instream data SYSIN when using DB2 utility to call PGM - ACCEPT. FROM PARAM when Exec Program
Mainframe Analyzer - Cobol	The following syntax is now supported: ACCEPT verb for processing data passed as input to Cobol programs via SYSIN. Data passed as input to Cobol programs via PARM.

SAP/ABAP Analyzer - Configuration change to increase analysis performance	A change has been to the SAP/ABAP Analyzer in order to improve analysis performance (execution time) particularly for very large analyses. For those upgrading to 8.3.21 and for new "out of the box" installations, in the following file: <INSTALLDIR>/configuration/AMT/AMTJobConfig_ABAP.xml, the following line: <analyzer name = "ABAP Analyzer" showProgress = "false" maxMem = "1000" maxInstancesForFlat64bits = "200000"/> has been replaced with: <analyzer name = "ABAP Analyzer" showProgress = "false" maxInstancesForFlat64bits = "400000"/>. If you are analyzing large SAP/ABAP projects and regularly find that analysis execution time is very long or gets stuck, CAST recommends gradually increasing the value of maxInstancesForFlat64bits to a point where performance is acceptable.
CAST Delivery Manager Tool - Exclusion rule changes	A change has been made in the CAST Delivery Manager Tool to the exclusion rule Exclude Eclipse project located inside the output folder of another Eclipse project. In previous releases this exclusion rule in fact addressed two different things: projects located inside the output folder of another Eclipse project projects that share the name of another Eclipse project To provide more flexibility, this rule has now been split in to two separate rules to address both exclusion scenarios handled by the original rule, as follows: "Exclude Eclipse project located inside the output folder of another Eclipse project" - Same name as in previous releases but this rule no longer excludes projects that share the name of another Eclipse project, Enabled by default, Same position as prior to the upgrade. "Exclude Eclipse project sharing the name of another Eclipse project" - New rule to address this specific scenario, enabled, same position as original rule prior to the upgrade to ensure consistency of results.
User Input Security - improved support of ASP.NET	User Input Security is now able to detect security violations in ASP.Net Core, ASP.Net MVC and ASP.Net MVC Core applications.
User Input Security - main/Main methods	User Input Security now takes into account arguments of main/Main methods (java / C# / VB.Net) as entry-points.
User Input Security - Apache Struts 2	User Input Security is now able to detect security violations in Apache Struts 2 applications.
User Input Security - NoSQL injections	NoSQL injections for applications using MongoDB/SpringData for Java can now be detected. Results are provided via the rule 8418 - Avoid NoSQL injection.
CAST Transaction Configuration Center	Saving empty transaction objects and Assessing Function Points for empty Transactional Functions based on non-empty Transactional Functions - see <a href="https://doc.castsoftware.com/display/AIPCORE/8.3.22+-+Additional+notes">https://doc.castsoftware.com/display/AIPCORE/8.3.22+-+Additional+notes</a> .

## Resolved Issues

Customer Ticket Id	Details
16341	DMT will unexpectedly exclude projects which do not match the exclusion rule.
22067	DMT will unexpectedly exclude projects which do not match the exclusion rule.
17599	On Rules Doc site, links in section "Reference" are broken for rule "Avoid catching an exception of type Exception, RuntimeException, or Throwable".
18329	While viewing Source code for database objects in the Engineering Dashboard, source code is not visible because the SQL file is too big.
20031	Unable to save changes in CAST-MS until pointer is outside the text box. CAST-MS was closing without any Pop-up, due to which the user would miss to notice that the changes were not saved in CAST-MS.
20774	While accepting the version in CAST MS, after having delivered a version with AIC Portal in CLI: accepting the delivery fails with an error "The program Version Report has not ended correctly" when a version is delivered through Source code automation Script.
21338	While comparing the .src file generated by the extractor and .ddl generated by a Database Management Tool: Inconsistencies observed between the two files, which suggests only a display issue in the .src files.
21543	When looking at the results of the rule "Never truncate data in MOVE statements - 7688: false positive violations of the rule are seen.
21545	While editing simulated grade in Action Plan Optimizer (APO): not able to calculate simulated grade in Action Plan Optimizer (APO).
21583	While entering the path to the CAST AIP installation folder. The CASTUpgrade_Config.txt file has a incorrect setting for the CAST_HOME Variable. (As per the documentation the variable should not end with back slash)
21604	Report generation fails in Dashboard, showing corrupt data in the database.

21663	When setting a delivery as the current version in the CAST Management Studio. The following error is displayed: "value too long for type character varying(255)" for the column "compilationconstants" in CMS_NET_Project table in management schema.
21698	When trying to validate or ignore a link using Dynamic Link Manager in CAST-MS. An error is thrown (SQL Error: ERROR: relation ""fusacc" " does not exist) but this error is not displayed in the Dynamic Link Manager task dialog box. The error is only visible in the log.
21894	In DMT, after running packaging, delivery and set as current version for a project that includes WSDL files. Two analysis units are created in the CAST Management Studio referring to the same WSDL file.
22051	When the APO (Action Plan Optimizer) is launched. (And a module is accessed, the issue is observed). Mismatch in 'Original Grade' and 'Simulated Grade' column values.

## 8.3.20

### Feature Improvements

Summary	Details
Analysis result save process has been optimized	The internal mechanism that is used to save analysis results in the CAST AIP schemas has been optimized and improved in this release of AIP. The goal of this optimization has primarily been to introduce more rigorous controls on the data that is saved to reduce inconsistencies and therefore to increase the overall accuracy of CAST AIP. In addition, performance has been stabilized. As a result of this optimization, some small changes in analysis results are to be expected when performing a new analysis/snapshot post-upgrade on unchanged source code, for example: Some objects, links, properties and bookmarks that flag the location of rule violations in the source code are now more rigorously checked and therefore some items may no longer be saved, notably for Universal Importer jobs, improving accuracy. Results of metrics calculated by the Metrics Assistant may be impacted (values may be higher or lower), improving accuracy. 7962 - Avoid direct or indirect remote calls inside a loop: previously some violations of this rule were not saved - these are now saved, improving accuracy.
CAST Server Manager - CLI	The -MODIFY_COMBINED command ( <a href="https://doc.castsoftware.com/display/DOC83/Automating+CAST+Server+Manager+installation+tasks">https://doc.castsoftware.com/display/DOC83/Automating+CAST+Server+Manager+installation+tasks</a> ) has been optimized to improve performance when using the command to Install new extensions, upgrade existing extensions or deactivate existing extensions to an existing combined installation (Management, Analysis and Dashboard Service schemas) - equivalent to the Manage Extensions option in the GUI.
Mainframe IMS/DC - support for links between Cobol Programs and IMS Transactions	CAST AIP 8.3.20 introduces support for links between Cobol Programs and IMS Transactions for IMS/DC (Data Communications). See <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe+--+IMS+DC+support">https://doc.castsoftware.com/display/TECHNOS/Mainframe+--+IMS+DC+support</a> .
Mainframe - IMS/DB - link type changes	Links between Cobol paragraphs/sections and DB/GSAM/ALT PCB when using DLI function have been updated as follows: OPEN/CLSE (only for GSAM): accessOpenLink, accessCloseLink. DLET: UseDeleteLink. GU/GHU, GN/GHN, GNP/GHNP, INQY: UseSelectLink. ISRT: UseInsertLink. REPL: UseUpdateLink. Other dli calls: useLink.
Mainframe - Avoid unchecked return code (SQLCODE ) after EXEC SQL query (7690)	Several fixes have been applied to the rule "Avoid unchecked return code (SQLCODE) after EXEC SQL query (7690)" to reduce the number of false violations reported: Correcting a situation where the rule is falsely violated when a paragraph contains multiple paragraphs called via IF clauses and where each of the called paragraphs contains SQL statements and where the SQL statement is checked from the parent paragraph. Correcting a situation where the rule is falsely violated when the SQL statement is contained in parentheses. Correcting a situation where the rule is falsely violated when the SQL statement is contained inside an IF statement of a PERFORM paragraph.
Mainframe - Never truncate data in MOVE statements (7688)	Fixes have been applied to the rule Never truncate data in MOVE statements (7688) to reduce the number of false violations reported.
Mainframe - CICS Return code should be checked (8162)	Fixes have been applied to the rule CICS Return code should be checked (8162) to reduce the number of false violations reported when the check statement is called via an IF statement in a variable.

Mainframe - JCL Symbol coverage	Improved coverage for JCL Symbol resolution: Support for EXEC Procedures or PGMs containing "&" such as "NAME1&VAR2". Support for the following situation: JOBS containing VAR1 = X and PROCs containing VAR1 = DEFAULT VALUE - X will not be overridden, and the value in JOB is taken as a priority.
CAST Transaction Configuration Center - GUI update for external end-points	An update has been made to the GUI of the CAST Transaction Configuration Center to allow users to see if an end point is external when checking the datafunction called by a transaction in a new column called Scope. For all datafunctions the scope is always "Application", but for end-points the scope can be "External" or "Application".
User Input Security - improved SecurityAnalyzer.log	The SecurityAnalyzer.log has been improved to list the number of distinct flaws found for each analyzed target. For example, "Distinct=" has been added: 2020-01-08 14:15:52,238 [1] DEBUG Analyzed target: 369/1941. Found=2, Distinct=1. Steps=128.
User Input Security - support for bsh. Interpreter. eval	Added support for bsh.Interpreter.eval ( <a href="http://www.beanshell.org/javadoc/bsh/Interpreter.html">http://www.beanshell.org/javadoc/bsh/Interpreter.html</a> ) as a target for code injection.
User Input Security - improvement to handling of constructors of System.IO.MemoryStream	Constructors of System.IO.MemoryStream are now handled correctly avoiding false positive violations to the rule "Avoid file path manipulation vulnerabilities (7752)".
User Input Security - improved coverage of database access methods from the .NET framework	Access to database methods of the .NET Framework are now handled more accurately. As a consequence, some false positives may be removed and new true positives may be found for the rule "Avoid SQL injection vulnerabilities (7742)".

## Resolved Issues

Customer Ticket Id	Details
18889	While calculating metrics (after completion of analysis). Error during run metrics calculation.
19655	False violations are being reported on constructors of the System.IO.MemoryStream class when running a User Input Security analysis.
20581	While doing JEE analysis and the source code path is very long. Analysis fails during the objects comparison step.
20706	While viewing the rule description: "Avoid Tables without Primary Key - 8082". The quality rule description is not accurate.
20960	While using the DMT to perform an HTTP Maven extraction. The DMT fails with "java.lang.OutOfMemoryError: Java Heap space" error, due to lack of memory during the packaging phase.
21028	While viewing the snapshot. Wrong AFP (Automated Function Point) number shown in Health Dashboard. After the snapshot, the number for AFP shown in Health Dashboard is different from the one in CED or TCC.
21184	When looking at the results of the rule Avoid unchecked return code (SQLCODE) after EXEC SQL query (7690). False violations are seen when a paragraph contains multiple paragraphs called via IF clauses and where each of the called paragraphs contains SQL statements and where the SQL statement is checked from the parent paragraph.
21239	While using CAST Transaction Configuration Center, an issue was observed due to DEDOUBLE function. Same transaction was displayed with two status (ADDED and DELETED).
21337	When simulated grade is changed from 1 to 4. Negative values are displayed in Action Plan Optimizer (APO). In APO, when the simulated grade was 1, there was no issue with the simulated violation count. When the simulated grade was set to 4, it resulted in a negative simulated violation count.

21386	While using the Action Plan Optimizer (after taking the snapshot). Difference in simulated and original score. In APO, original grade and simulated grade should be identical.
21412	After upgrading to 8.3.15, violations were not triggered for the QR: "Persistent class method's equals() and hashCode() must access its fields through".

## 8.3.19

### Feature Improvements

Summary	Details
Mainframe Analyzer - IMS/DC support introduced	Support for IMS/DC (Data Communications) has been introduced. See <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++IMS+DC+support">https://doc.castsoftware.com/display/TECHNOS/Mainframe++IMS+DC+support</a> . As a result, some changes have been implemented: the Mainframe Discoverer ( <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe+Discoverer">https://doc.castsoftware.com/display/TECHNOS/Mainframe+Discoverer</a> ) will detect a project (and therefore automatically create an Analysis Unit) for each *.tra file discovered in a folder. See <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Application+qualification+specifics">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Application+qualification+specifics</a> for more information about how to generate this file type using JCL. .tra files have been added to the list of files that will be automatically analyzed - see for example <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+configuration">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+configuration</a> . New object types will be resolved for "IMS Transaction File" and "IMS Transaction" - see <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+results">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Analysis+results</a> . A new option (IMS DC) has been added to the Delivery Manager Tool when delivering a PDS dump file, specifically to collect IMS DC related items.
Mainframe - JCL	Support for SQL embedded in INZUTILB and DSNTIAUL items has been added.
User Input Security - support for Ektorp Java API for CouchDB	NoSQL injections for applications using Ektorp Java API for CouchDB can now be detected.
User Input Security - support for LightCouch for Java	NoSQL injections for applications using LightCouch for Java can now be detected. Results are provided via the rule "8418 - Avoid NoSQL injection".
User Input Security - improved coverage of logger methods	Methods like "logError", "logInfo", etc. used in loggers are now automatically taken into account.
User Input Security - improved logs	Where a blackbox contains a duplicated type (according to their mangling), the log of the tool will contain more detailed information about the issue (the name of the duplicated type or the name of the duplicated blackbox, etc.).
User Input Security - improved handling of duplicate paths	In previous releases some violations were removed if other violation paths were found in other files with a similar position of the starting path and the ending path (same row and same column for both). The algorithm for detecting these duplicate paths has now been rewritten to provide more accurate results.
User Input Security - support for NoSQL - Azure Cosmos DB (.NET)	NoSQL injections for applications using Azure Cosmos DB for .NET can now be detected. Results are provided via the rule "8418 - Avoid NoSQL injection".
User Input Security - support for NoSQL - Azure Cosmos DB (Java)	NoSQL injections for applications using Azure Cosmos DB for Java can now be detected. Results are provided via the rule "8418 - Avoid NoSQL injection".

User Input Security - improved detection of targets of the method java.io.Console.format	The targets of the method java.io.Console.format - String fmt, Object... args etc. - are now correctly detected.
--	--

## Resolved Issues

Customer Ticket Id	Details
19530	When running a snapshot, the "Run metrics calculation" step fails with the error : "Unexternalized Exception - Message is 'access violation' ".
19860	When attempting to use the CAST Extension Downloader. ExtensionDownloader.exe crashes with the following error: Root element missing.
20087	CAST Transaction Configuration Center displays added and deleted objects for overloaded PowerBuilder methods even though the source code is unchanged since the previous snapshot.
20417	In a JEE project discovered by the DMT, sometimes the same directory reference is shared between JARs, XML and/or Properties. In the corresponding analysis unit, a shared reference is only configured once, for the latest section amongst: 1) JARs 2) XML files 3) Properties files.
20562	When looking at the results of successive snapshots with regard to Complexity Factor values. Inconsistency in Complexity Factor, AAFP and AEP values.
20687	While looking at the results of .NET related rules. Inconsistency in the total number of violations reported at technical criterion level and the total number for all contributing rules. This is due to a bug where VB.NET Property Setter objects were not being included correctly in total object counts for related rules.
20744	While running analysis, Universal Analyzer analysis running for a long time (2-days).

## 8.3.18

### Feature Improvements

Summary	Details
Technology support changes - SAP ABAP	The following syntax is now supported: CALL TRANSACTION...WITH AUTHORITY-CHECK USING.
.NET - Procedure Call Depth	The default value for the option Procedure Call Depth (which limits the number of intermediate values that the Inference Engine can resolve in order to obtain the type of the object that is being searched for) - see <a href="https://doc.castsoftware.com/display/TECHNOS/.NET+-Analysis+configuration">https://doc.castsoftware.com/display/TECHNOS/.NET+-Analysis+configuration</a> - has been changed to 300 (from 3000) for all Applications newly onboarded with 8.3.18. This change has been made to improve the .NET analysis duration time. For Applications that are upgraded from a previous release of AIP to 8.3.18, the previous value for this option will be retained to avoid impacting analysis results.
CAST Transaction Configuration Center - specific usage of Excluded Items	Data functions / transaction functions will still contribute to values in the AFP section in the following situations: 1) The setup configuration rule matching the(se) object(s) is no longer present. 2) The setup configuration rule has changed and no longer matches the objects. This is because these Data functions / Transactions have already been calibrated (i.e. merged / deleted / ignored) and a Compute action will not remove these items from the values in the AFP section to prevent losing the specific calibration that has been applied. Therefore, if you need to prevent these objects contributing to values in the AFP section, you can: 1) Create an excluded-item rule to exclude these items 2) Run the Compute action 3) Disable or remove the excluded-item rule you created.

CAST Transaction Configuration Center - Change in behavior with regard to loss of transaction IDs	In previous releases of CAST AIP, Added/Deleted objects would be visible in the following situation: If an entry point of a valid transaction is missing in more than two consecutive snapshots, then the transaction ID is lost. As a consequence when the missing entry-point object re-appeared in a subsequent snapshot, CAST AIP was not able to recover the transaction ID and a new transaction ID was associated to the entry point. If the intermediary snapshots were then deleted, CAST AIP recorded an Added/Deleted of the transaction because CAST AIP sees that the transaction has a new ID and the previous ID is no longer present in the snapshot. The behaviour of CAST AIP in this situation has been changed - the previous transaction ID will be re-used when the missing entry-point object re-appears in a subsequent snapshot. And so when the intermediary snapshots are deleted, the transaction will be seen as Unchanged (if there are no changes in the transaction's details ) or Modified (if there are changes in the transaction's details).
User Input Security - support of org.owasp.encoder library	Methods from the "org.owasp.encoder" library have been added to the list of libraries that are automatically taken into account for Sanitization.
User Input Security - Avoid hard-coded credentials (8222) for .NET	The rule Avoid hard-coded credentials (8222) has been updated to include support for detecting hard-coded credentials in the PasswordDeriveBytes Class ( <a href="https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.passwordderivebytes?view=netframework-4.8">https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.passwordderivebytes?view=netframework-4.8</a> ).
Improvements to CAST-DatabaseExtractionRenamingTool.exe	The CAST-DatabaseExtractionRenamingTool.exe tool that is used to mitigate the impact on analysis results when databases or schemas move from one Server to another or from one Instance to another has been enhanced to support renaming for database extractions performed on Microsoft SQL Server and Sybase ASE.

## Resolved Issues

Customer Ticket Id	Details
12651	While running a .NET analysis with User Input Security analysis enabled. The devirtualization phase is taking a long time to complete.
18394	The snapshot generation used to get stuck for 24hrs in the following step: "Transfer Sources,positions,Bookmarks into Dashboard service". After the fix, there is great improvement in the performance. Now the snapshot generation of the above step is completed in 2 seconds.
18421	When renaming an application in Chinese. Incorrect application name display in CMS after renaming application in Chinese.
18617	While generating snapshot using CLI. After snapshot failure on Jenkins, CMS doesn't prompt to purge the existing snapshot before taking new one.
19936	The Menu bar of the Server Manager is in French language after launching.
20067	When attempting to run an ABAP analysis. Unsupported syntax errors are displayed for the syntax "CALL TRANSACTION...WITH AUTHORITY-CHECK USING".
20101	Error in ADDED and DELETED objects in AEP counts, when a snapshot is deleted.
20342	TCC computation is getting stuck at Finalizing function Point Computation Step.
20393	Inconsistency in the number of violations displayed in Engineering dashboard for the rule "Package size control (4718)".
20394	Inconsistency in the number of violations displayed in Engineering dashboard for the rule "Avoid catching an exception of type Exception, RuntimeException, or Throwable (7862)".
20399	Inconsistency in the number of violations displayed in Engineering dashboard for the rule "Avoid unreferenced Functions (7860)".
20400	Inconsistency in the number of violations displayed in Engineering dashboard for the rule "Avoid using GOTO statement (7816)".
20444	Inconsistency in the number of violations displayed in the Engineering dashboard for the rules "Avoid Namespaces with High Efferent Coupling (CE) (7262)" and " Avoid namespaces with High Afferent Coupling (CA) (7264)".

## 8.3.17

## Feature Improvements

Summary	Details
CAST Extension Downloader	Some changes have been made to switch extension downloads to the "next generation" CAST Extend ( <a href="https://extend.castsoftware.com">https://extend.castsoftware.com</a> ). This new CAST Extend is a replacement for the existing CAST Extend which will be phased out in due course. Note that to use <a href="https://extend.castsoftware.com">https://extend.castsoftware.com</a> , you will need to register a new account ( <a href="https://extend.castsoftware.com/register">https://extend.castsoftware.com/register</a> ) - however, accounts from the existing CAST Extend service will be transferred in over the coming weeks.
CAST Extension Downloader - Installing CAST AIP 8.3.17 from scratch	When installing CAST AIP 8.3.17 from scratch when no previous release of CAST AIP exists, the "extendng.castsoftware.com" server will be pre-configured for extension downloads (the server will be ticked and enabled). Note that you can manually add the URL of the existing CAST Extend service if you prefer to use it, however, you should bear in mind that this service will be phased out in due course.
CAST Extension Downloader - Installing CAST AIP 8.3.17 when a previous release of CAST AIP already exists	When installing CAST AIP 8.3.17 and a previous release of CAST AIP already exists (more specifically if the %PROGRAMDATA%\CAST\CAST\Extensions\ServerList.xml file exists) then the following will occur: 1) <a href="https://extendng.castsoftware.com/api">https://extendng.castsoftware.com/api</a> will be added as CAST ExtendNG and will be ticked and enabled 2) <a href="https://extend.castsoftware.com:443/v2/api/v2">https://extend.castsoftware.com:443/v2/api/v2</a> will be deleted 3) All other servers will remain as they were previously. Note that you can manually add the URL of the existing CAST Extend service if you prefer to use it, however, you should bear in mind that this service will be phased out in due course.
CAST Transaction Configuration Center - Set/layer creation with Caller-Of and Callee-Of blocks	It is now possible to create Caller-Of and Callee-Of blocks using multiple link types. Previously, only one single link type could be selected. Configurations built with this new feature cannot be used with CAST Transaction Configuration 8.3.16 (i.e. importing a .TCCSetup file that contains this new configuration). Erroneous results will be produced.
User Input Security - support for MongoDB for Java	NoSQL injections for applications using MongoDB for Java can now be detected. Results are provided via the rule 8418 - Avoid NoSQL injection.
User Input Security - Name of rule changed - Sensitive cookie in HTTPS session without 'Secure' attribute (8240)	The rule Sensitive cookie in HTTPS session without 'Secure' attribute (8240) has been renamed as Avoid using unsecured cookie (8240).
User Input Security - SpringMVC technology - total checks less than failed checks (violations)	A bug causing the total number of checks to be reported as lower than the total number of failed checks (i.e. violations) for Applications containing SpringMVC technology has been fixed therefore improving accuracy.
User Input Security - Improvement to Avoid HTTP response splitting (7740) rule	The rule Avoid HTTP response splitting (7740) computed by the User Input Security has been improved: the full path of related violations is now computed thus improving bookmark accuracy.
User Input Security - java.io.ObjectInputStream methods handled	java.io.ObjectInputStream methods are now automatically taken into account.
User Input Security - Improvement to SpringMVC regression introduced in 8.3.16	During the analysis of an application using Spring MVC, a blackbox is generated by the SpringMVC extension ( <a href="https://doc.castsoftware.com/display/TECHNOS/Spring+MVC">https://doc.castsoftware.com/display/TECHNOS/Spring+MVC</a> ), however, this blackbox was ignored during a User Input Security analysis. As a result, some violations were not found. This bug has been fixed improving accuracy.
User Input Security - Support for CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	Support has been introduced for CWE-601: URL Redirection to Untrusted Site ('Open Redirect') - <a href="https://cwe.mitre.org/data/definitions/601.html">https://cwe.mitre.org/data/definitions/601.html</a>
User Input Security - Avoid log forging vulnerabilities (8044) - total checks less than failed checks (violations)	A bug causing the total number of checks to be reported as lower than the total number of failed checks (i.e. violations) has been fixed therefore improving accuracy.

## Resolved Issues

Customer Ticket Id	Details
19102	Failed checks is greater than Total checks for CWE-117: Avoid log forging vulnerabilities.
19244	The compute snapshot step is taking a very long time to complete due to the volume of rows generated for computing the differences between the two snapshots.
19281	After upgrade to 8.3.x (from 8.1.x), generation of post-upgrade snapshot and comparison of the results. Many violations that were detected in AIP 8.1.x for the rule "Avoid declaring throwing an exception and not throwing it - 4656" are no longer visible in AIP 8.3.x.
19401	While viewing the results of a snapshot in the CAST dashboards. The total number of failed checks is greater than total number of checks.
19522	If user has AIP build on mapped or network drive. Installing new schema gives error - "duplicate key value violates unique constraint "uidx_da_entity""
19607	If user has AIP build on mapped or network drive. Getting Error while doing upgrade: "more references than expected"
19761	Launch a snapshot on a Powerbuilder application. Analyzed source code is not available in Engineering Dashboard/Imaging System.
19790	Snapshot generation gets stuck. (Configure snapshot step)

## 8.3.16

### Feature Improvements

Summary	Details
Support of PostgreSQL 10 for storage	Support has been introduced for PostgreSQL 10 and 11 (64bit) as storage, i.e. AIP schemas can now be created on these versions and analyses will run as expected.
Mainframe Analyzer - support for IBM MQSeries	In CAST AIP 8.3.16, Mainframe Analyzer supports the publisher/subscriber mode and point-to-point mode for IBM MQSeries. Publisher/Subscriber objects will be generated and Call links between Cobol objects and IBM MQ objects and between IBM MQ objects and Cobol objects will be generated by the Web Services Linker extension ( <a href="https://doc.castsoftware.com/display/TECHNOS/Web+Services+Linker">https://doc.castsoftware.com/display/TECHNOS/Web+Services+Linker</a> ) - you must ensure that v. 1.6.8 of this extension is installed, otherwise no links will be generated. You can find out more information about this support in <a href="https://doc.castsoftware.com/display/TECHNOS/Mainframe++Technical+notes#MainframeTechnicalnotes-IBMMQ">https://doc.castsoftware.com/display/TECHNOS/Mainframe++Technical+notes#MainframeTechnicalnotes-IBMMQ</a> .
CAST Database Extractor	The CAST Database Extractor ( <a href="https://doc.castsoftware.com/display/DOCCOM/CAST+Database+Extractor">https://doc.castsoftware.com/display/DOCCOM/CAST+Database+Extractor</a> ) now supports: (by reference) the extraction of schemas on Oracle 18c and above in line with Oracle's updated release cycle, however the extractor will handle the schemas as Oracle 12c schemas and no new syntax or features introduced in these newer releases is supported. Case sensitive passwords (introduced in Oracle 12c R2).
User Input Security - rule documentation changes	For several User Input Security related rules, the Total field has been updated to state "Number of potentially vulnerable methods" instead of "Number of methods calling user input methods". This is to better reflect what is returned by the rule. In addition, Links to external references have been updated for several User Input Security related rules to provide more up-to-date references.
SAP / ABAP - CX_ROOT" should not be used in TRY .. CATCH.. ENDTRY block (8412)	For the rule "CX_ROOT" should not be used in TRY .. CATCH.. ENDTRY block (8412)", the parent technical criterion for this rule was incorrectly set to 61020: Programming Practices - Modularity and OO Encapsulation Conformity, but it has been changed to 61014: Programming Practices - Error and Exception Handling.
SAP/ABAP - source code bookmarks implemented	Bookmarks indicating the position of violations in the source code have been implemented for the following SAP/ABAP rules: 7130, 7524, 7528, 7530, 7532, 7536, 7538, 7544, 7592, 7594, 7666, 7672, 7788, 7806, 7808, 7810, 7820, 7822, 7882, 7902.
.NET - rule changes	The following multi-techno rules have been disabled in 8.3.16 specifically and only for .NET technology and will no longer be triggered during an analysis. These rules often generated a large amount of false positive violations: Avoid unreferenced Classes - 7832, Avoid unreferenced Data Members - 7912, Avoid unreferenced Methods - 7908.
Dynamic Links rule files	Dynamic Links rule files now function with SAP BusinessObjects and SAP PowerBuilder analysis results.

Changes to the structure of the Dashboard and Analysis Services schemas - FP_LINK_INFO table (new)	Data (links with IDs from 11000 to 11006) related to CAST Transaction Configuration Center data functions and transactions that was previously stored in these two tables will now be stored in a new table called FP_LINK_INFO. This table now contains all object details of transactions/data functions. It has exactly the same structure as DSS_LINK_INFO.
Changes to the structure of the Dashboard and Analysis Services schemas - Impact on Analysis Services schema	Details of transactions and data functions are now sent to a new table called DSS_FPLINKS (previously DSS_LINKS was used).
Changes to the structure of the Dashboard and Analysis Services schemas - transfer from Analysis to Dashboard Service schema	The links in DSS_FPLINKS in the Analysis Service schema are sent to the Dashboard Service schema via a new table called DSS_IN_FPLINKS (previously DSS_IN_LINKS was used).
Changes to the structure of the Dashboard and Analysis Services schemas - Upgrade and impact	This change is handled by the CAST upgrade process and does not require any manual steps. All occurrences of link_type_id between 11000 and 11006 will be: 1) Moved from DSS_LINK_INFO to FP_LINK_INFO 2) Removed from both DSS_LINK_INFO and DSS_LINKS. If you have custom scripts that fetch data from any of the existing tables, please ensure that you update these scripts yourself.
Changes to the structure of the Dashboard and Analysis Services schemas - impact on Dashboard Services schema	The data related to details of transactions and data functions are now stored in a new table called FP_LINK_INFO (previously DSS_LINK_INFO was used).

## Resolved Issues

Customer Ticket Id	Details
14882	When attempting to run a mainframe analysis. Anarun crashes while attempting to process a .cbl file.
14918	While running DMT for packaging a java application. The following warning is displayed: "cast.dmt.engine.foldertree.containerScannerFailure"
15791	When attempting to analyze a .NET application. The analysis is hanging during the Comparing Object step due to the duplicate objects caused by 2 .csproj pointing to the same source code.
16120	When attempting to apply a DLM rule file on SAP BusinessObjects results - the DLM rule file does not review any links - i.e. all results are ignored.
16639	When attempting to run a Mainframe analysis. The analysis fails with the error "Unexternalized exception - Message is 'access violation'."
17065	When looking at the log files following a Mainframe analysis. Difficult to work out which copybook (when the same one has been identified more than once in the Application) has been used for the analysis.
17183	When looking at the results of a Mainframe analysis, with regard to the rule "Avoid OPEN/CLOSE inside loops - 7218". A false link between two objects is causing a false violation of the rule.
17220	When looking at the results of a Mainframe analysis. An incorrect Cobol program object called "TO" is created for the "MOVE PROGRAM-ID ... TO ..." syntax found in cobybook files. No object should be created at all.
17233	When looking at the results of a Mainframe analysis, specifically with regard to the rule "Avoid unchecked return code (SQLCODE) after EXEC SQL query - 7690". False positive violations are reported for this rule when SQLCODE is checked outside perform statement of a paragraph.
17365	When attempting to use a Dynamic Links rule file with PowerBuilder analysis results. The rules described in the Dynamic Links rule file are ignored.
17366	When looking at the results of a Mainframe analysis. Many Cobol Transaction objects are created with names containing special characters such as *, / etc.

17613	When creating a Reference Pattern in the CAST Management Studio and attempting to use the "Enable replacement" option. The "Enable replacement" option does not replace the words as expected. when attempting to replace a "\" (backslash).
17783	The snapshot generation process is hanging during the run consolidation step.
17816	When looking at the results of a Mainframe analysis, specifically with regard to the rule "Avoid unreferenced Sections and Paragraphs - 7290". The analyzer does not correctly handle the syntax FETCH / END-FETCH (it is treated as paragraph) and therefore causes a false violation of the rule.
18112	The snapshot fails during the MAV2 step with the error message: Unexternalized exception - Message is 'access violation ' Failed to run service ILocalMetrics
19440	The snapshot fails during the MAV2 step with the error message: Unexternalized exception - Message is 'access violation ' Failed to run service ILocalMetrics
18221	False positive violations are generated for the rule "Prefer using indexes instead of subscripts - 8142" even though Indexing was used instead of Subscripts.
18236	When looking at the results of the rule "Avoid "SELECT *" queries (7344)". The violations reported for this rule are duplicated by the rule "Avoid "SELECT *" or "SELECT SINGLE *" queries" (7530).
18348	Module trending for an application in AAD always returns with "unexpected error" as rest-api doesn't accept special characters(/,&) in module names.
18508	When using a Dynamic Link Rule file to automatically ignore specific link types during an analysis. The rules file does not automatically ignore "uselinks" links.
18570	CICS Maps objects are not handled correctly - objects are displayed as "Unknown" and the same object is displayed multiple times impacting link creation.
18635	When looking at the results of a Mainframe analysis specifically with regard to the rule "Never truncate data in MOVE statements - 7688". False violations are reported for this rule when the variables have subordinate items and the comparison is based on a block.
18652	A different number of violations is showing in the "Risk Model" and in "Application Component" tiles. The values in both should be the same. The issue is due to the fact that CAST_DotNet_PropertyCSharp objects are marked as synthetic, whereas their associated getters /setters are not.
18660	Using Server Manager CLI to install an extension and the installation fails for whatever reason. No non-zero error code is returned by Server Manager CLI.
18670	When a Management Database is locked by CAST MS (after having enabled the lock) by user A. User B then opens a new CAST MS session. An error message is raised incorrectly stating that user A has CAST MS open.
18711	When attempting to package Maven based JEE source code. Missing JAR files in the DMT packaging results, despite the fact that the JAR files are present in the Maven repository.
18854	When generating a snapshot. The procedure DSSEXT_BUILD_OBJ_STATUS takes a long time to complete.
18873	When analyzing a Mainframe application in CAST AIP 8.3.x after upgrade from 8.2.x with no change in source code. The analysis time has increased 7-fold.
18947	Using the DMT and attempting to delete a package from V2 (cloned from V1). The package is deleted, but an error is displayed: "The program validation has not ended correctly (2001)"
18959	When installing CAST AIP and recording the settings in a .iss file. The .iss files does not store the correct path for the CAST_DEFAULT_DELIVERY_DIR variable chosen during the installation and instead will record the path given in the CastGlobalSettings.ini file.
19041	When looking at the results of a post upgrade (8.2.x > 8.3.x) consistency analysis on unchanged source code. The checksum of some objects has changed, therefore impacting the results (some objects are marked as modified even though they have not been changed).
19054	When looking at the parent Technical Criterion for the rule ""CX_ROOT" should not be used in TRY .. CATCH.. ENDRY block - 8412". This parent technical criterion for this rule is set to "61020: Programming Practices - Modularity and OO Encapsulation Conformity", but it should be changed to "61014: Programming Practices - Error and Exception Handling".
19091	Snapshot is taking longer than expected to complete the procedure ADG_COMPUTE_VIOLATION_STATUSES.
19126	When attempting to run a Mainframe analysis. The analyzer crashes with errors similar to: - Mainframe.14: Potential mismatch between the program and the PSB '<object_name>'. The PCB number 3 has not been found. - Job execution Internal exception occurred during processing listener <item>
19132	When attempting to analyze a C++ application. The following error is displayed in the log: BuildAll.Sources: Missing Sources
19261	When attempting to generate a snapshot. The snapshot runs and does not complete.
19297	Snapshot is taking longer than expected to complete the procedure ADG_COMPUTE_VIOLATION_STATUSES.
19439	When attempting to run a Mainframe analysis. Anarun crashes when analyzing certain Cobol files.

19472	When looking at the source code delivery log in the DMT. The DMT cannot find the parent maven artifact of a specific child maven artifact when other child maven artifacts that reference the same parent artifact using a different version number.
19500	When attempting to use the Search in Code tool in CAST Enlighten. CAST Enlighten crashes when running the tool.
19537	When looking at the source code delivery log in the DMT. The DMT cannot find the parent maven artifact of a specific child maven artifact when other child maven artifacts that reference the same parent artifact using a different version number.