



Update Summary for wso2das - 3.1.0 1508286726036

This document contains details of 78 update(s) installed into your wso2das-3.1.0 distribution. There are 34 security update(s). WSO2 strongly recommends to use this updated product for production as soon as possible.

List of security updates

- [WSO2 Carbon 4.4.X Update 2016-09-19](#)
- [WSO2 Carbon 4.4.X Update 2016-10-24](#)
- [WSO2 Carbon 4.4.X Update 2016-11-16](#)
- [WSO2 Carbon 4.4.X Update 2016-12-02](#)
- [WSO2 Carbon 4.4.X Update 2016-12-06](#)
- [WSO2 Carbon 4.4.X Update 2016-12-07](#)
- [WSO2 Carbon 4.4.X Update 2016-12-07](#)
- [WSO2 Carbon 4.4.X Update 2016-12-21](#)
- [WSO2 Carbon 4.4.X Update 2016-12-23](#)
- [WSO2 Carbon 4.4.X Update 2017-01-06](#)
- [WSO2 Carbon 4.4.X Update 2017-01-12](#)
- [WSO2 Carbon 4.4.X Update 2017-01-19](#)
- [WSO2 Carbon 4.4.X Update 2017-02-27](#)
- [WSO2 Carbon 4.4.X Update 2017-02-28](#)
- [WSO2 Carbon 4.4.X Update 2017-02-28](#)
- [WSO2 Carbon 4.4.X Update 2017-03-01](#)
- [WSO2 Carbon 4.4.X Update 2017-03-02](#)
- [WSO2 Carbon 4.4.X Update 2017-04-03](#)
- [WSO2 Carbon 4.4.X Update 2017-04-04](#)
- [WSO2 Carbon 4.4.X Update 2017-04-06](#)
- [WSO2 Carbon 4.4.X Update 2017-04-06](#)
- [WSO2 Carbon 4.4.X Update 2017-04-17](#)
- [WSO2 Carbon 4.4.X Update 2017-04-17](#)
- [WSO2 Carbon 4.4.X Update 2017-04-21](#)
- [WSO2 Carbon 4.4.X Update 2017-04-28](#)
- [WSO2 Carbon 4.4.X Update 2017-04-28](#)
- [WSO2 Carbon 4.4.X Update 2017-05-07](#)
- [WSO2 Carbon 4.4.X Update 2017-06-03](#)
- [WSO2 Carbon 4.4.X Update 2017-07-07](#)
- [WSO2 Carbon 4.4.X Update 2017-07-10](#)
- [WSO2 Carbon 4.4.X Update 2017-08-17](#)
- [WSO2 Carbon 4.4.X Update 2017-09-01](#)
- [WSO2 Carbon 4.4.X Update 2017-09-07](#)
- [WSO2 Carbon 4.4.X Update 2017-09-28](#)

Following updates contain instructions. Please read them carefully and apply to your deployment if necessary.

- [WSO2 Carbon 4.4.X Update 2016-10-24](#)

- [WSO2 Carbon 4.4.X Update 2017-04-20](#)
- [WSO2 Carbon 4.4.X Update 2017-05-05](#)
- [WSO2 Carbon 4.4.X Update 2017-05-15](#)
- [WSO2 Carbon 4.4.X Update 2017-05-18](#)
- [WSO2 Carbon 4.4.X Update 2017-08-04](#)
- [WSO2 Carbon 4.4.X Update 2017-10-18](#)

WSO2 Carbon 4.4.X Update 2016-09-19

If the `autocomplete=false` is not been set in the password fields of html/jsp/etc.. pages browser will cache the password. This update will set that attribute where necessary in ui pages.

WSO2 Carbon 4.4.X Update 2016-10-14

This update is to solve the error which is occurring when adding new user in carbon console while having `MultipleAttributeEnable` property enabled in `user-mgt.xml` file.

Bug Fixes

- [IDENTITY-5213](#) - CLONE - Error occurred when creating a new user

WSO2 Carbon 4.4.X Update 2016-10-24

This update introduces a filter which is capable of applying cache-prevention headers to HTTP responses. The application of this filter would prevent sensitive information being cached in web browsers, proxies and other intermediate network devices. By default the following cache-prevention headers would be added to HTTP responses. `Cache-Control : no-store, no-cache, must-revalidate`
`Pragma : no-cache Expires : 0`

Instructions

Do the following changes to `<CARBON_SERVER>/repository/conf/tomcat/carbon/WEB-INF/web.xml`:

a. Add the following configuration after the existing filters:

```
<filter>
<filter-name>URLBasedCachePreventionFilter</filter-name>
<filter-class>org.wso2.carbon.ui.filters.cache.URLBasedCachePreventionFilter</filter-class>
</filter>
```

b. Add the following configuration after the existing filter mappings:

```
<filter-mapping>
<filter-name>URLBasedCachePreventionFilter</filter-name>
<url-pattern>*.jsp</url-pattern>
</filter-mapping>
```

NOTE: Please make sure this is the last filter mapping configuration in the `web.xml` file.

WSO2 Carbon 4.4.X Update 2016-10-26

When events are published to a binary endpoint, event publisher opens a connection with DAS and maintain a session. This session expires each 30 minutes (by default) and recreates a session. During this procedure, A data endpoint exception arises from the client end. This update handles that issue and correctly wrap the exception as a session timeout exception, and recreates the session without a delay.

Bug Fixes

- [CANALYTCOM-8](#) - Getting DataEndpointException periodically - Unable to send events to the endpoint
-

WSO2 Carbon 4.4.X Update 2016-11-07

This update contains the fix for being not able to change the passwords when using email as username with Active Directory (which has username attribute as cn)

Bug Fixes

- [IDENTITY-5245](#) - Unable to change the passwords when using email as username with Active Directory (which has username attribute as cn)
-

WSO2 Carbon 4.4.X Update 2016-11-16

This update is given as a security fix to prevent access an unauthorized URL and read arbitrary file outside the JAR. This update is only compatible with products which using carbon-commons 4.5.4 tryit module.

WSO2 Carbon 4.4.X Update 2016-11-28

This update resolves the issue of NullPointerException which was caused due to not initializing primaryHazelcastConfig in HazelcastClusteringAgent while initiating custom membership schemes.

Bug Fixes

- [CARBON-16062](#) - PrimaryHazelcastConfig being null in initiateCustomMembershipScheme method
-

WSO2 Carbon 4.4.X Update 2016-12-02

Try it WSDL validation issues in <https://localhost:9443/carbon/tryit/index.jsp?region=region5&item=tryit>

WSO2 Carbon 4.4.X Update 2016-12-06

In some versions of the WSO2 Thrift data publisher clients, a vulnerability has been discovered where the password used for authenticating against the Thrift server is printed in the client logs. This update addresses that issue.

WSO2 Carbon 4.4.X Update 2016-12-07

Cross-site scripting vulnerabilities found in org.wso2.carbon.registry.common, org.wso2.carbon.registry.search

WSO2 Carbon 4.4.X Update 2016-12-07

Cross-site scripting vulnerabilities found in org.wso2.carbon.tenant.mgt.ui

WSO2 Carbon 4.4.X Update 2016-12-15

This update will add the registerTenantForTrustedUser method to the TenantSelfRegistrationService

Bug Fixes

- [CMTENANCY-11](#) - Missing method in TenantSelfRegistrationService
-

WSO2 Carbon 4.4.X Update 2016-12-21

This update will fix the existing xss vulnerability in the roles management ui component

WSO2 Carbon 4.4.X Update 2016-12-23

This update will fix the existing xss vulnerability in the messageflow component.

WSO2 Carbon 4.4.X Update 2016-12-26

SSO and SLO configuration for carbon server - Eventhough IdentityProviderSLOServiceURL is mentioned in authenticators.xml Destination value in SAML request is the SSO url not the SLO url.

Bug Fixes

- [IDENTITY-5356](#) - Issue in SAML Single logout url
-

WSO2 Carbon 4.4.X Update 2017-01-05

Encrypted JMS secured properties are still shown in plain text in the view mode. This update makes this text secure and after applying this update encrypted properties will not be shown as plain text.

Bug Fixes

- [CEP-1595](#) - Encrypted JMS secured properties are still shown as plain text in view mode.
-

WSO2 Carbon 4.4.X Update 2017-01-06

This update addresses reflected Cross-Site-Scripting vulnerability found in Event Simulator and Event Tracer as well as Reflected User-Interaction Cross-Site-Scripting Vulnerability found in Template manager components.

WSO2 Carbon 4.4.X Update 2017-01-12

This update will fix the existing xss vulnerability in the roles management ui component

WSO2 Carbon 4.4.X Update 2017-01-15

This update addresses the issue of Kafka input receiver getting crashed after receiving an invalid /malformed event.

Bug Fixes

- [CEP-1596](#) - Kafka receiver crashes after receiving an invalid event
-

WSO2 Carbon 4.4.X Update 2017-01-19

This update removes the WS-Security detailed error messages with internal details avoiding unnecessary information disclosure. If you need a detailed error message, add below property to `<CARBON_SERVER>/repository/conf/axis2/axis2.xml` inside `<axisconfig>`. `<parameter name="includeFullWSecurityExceptionMessage" locked="false">true</parameter>` Example For a service secured with Sign and Encrypt - X509 Authentication, Below are the detailed error message and non detailed error message Detailed error message: The signature or decryption was invalid; nested exception is: org.apache.xml.security.signature.XMLSignatureException: It should be divisible by four Original Exception was org.apache.xml.security.exceptions.Base64DecodingException: It should be divisible by four Non detailed error message after applying the update: The signature or decryption was invalid

WSO2 Carbon 4.4.X Update 2017-01-19

This update will avoid using plain text for JMS Secured Properties in JMS output adaptor.

Bug Fixes

- [CEP-1595](#) - Encrypted JMS secured properties are still shown as plain text in view mode.
-

WSO2 Carbon 4.4.X Update 2017-02-27

This update fix the security issue which password auto complete is not disabled by default for components `org.wso2.carbon.security.mgt.ui` and `org.wso2.carbon.user.mgt.ui`.

WSO2 Carbon 4.4.X Update 2017-02-28

This update fixes security vulnerabilities in ndatasource component: Cross Site Scripting (XSS), Unencoded characters, Password autocompletion

WSO2 Carbon 4.4.X Update 2017-02-28

This update upgrades the embedded tomcat version to 7.0.75 to mitigate security vulnerabilities present in the current embedded tomcat version used in the product. For more information on fixed vulnerabilities, please refer <https://tomcat.apache.org/security-7.html>

WSO2 Carbon 4.4.X Update 2017-03-01

Disable autocomplete for Password field in tenant addition page.

WSO2 Carbon 4.4.X Update 2017-03-02

Management console advancedSearch parameters might contain sensitive information (commentedUser) which will get logged in access_logs. Therefore, it is required to change search submission to POST in order to prevent logging sensitive information. This update will prevent logging sensitive information in access_logs.

WSO2 Carbon 4.4.X Update 2017-03-03

This update fixes an issue in applying custom themes using extensions in dashboard portal.

Bug Fixes

- [UES-1132](#) - Customizing portal using extensions, is not working
-

WSO2 Carbon 4.4.X Update 2017-03-09

This update will fix the issue in LengthWindow of size 0, when joining a stream with a table(which has inconsistency in data)

Bug Fixes

- [SIDDHI-30](#) - Issue in length window (#window.length(0))
-

WSO2 Carbon 4.4.X Update 2017-04-01

In DAS 3.1.0 and ML 1.2.0, ML data source doesn't support Microsoft SQL Server due to differences in the queries defined in ML. This update will fix the mentioned issue.

Bug Fixes

- [ML-321](#) - Machine Learning Database Scripts for Sql Server
-

WSO2 Carbon 4.4.X Update 2017-04-03

This update provides a fix for a potential authentication bypass security vulnerability detected in the management console for a protected page.

WSO2 Carbon 4.4.X Update 2017-04-03

This update solves following issues in gadget creation for Oracle, DB2, PostgreSQL and MSSQL server. 1. When show data button clicked an error occurred. 2. When go to configure chart step an error occurred. 3. Gadget preview and gadget after published to dashboard shows an empty one.

Bug Fixes

- [CDASHBOARD-8](#) - DAS configuration not working on Publisher Node for getting statistics
-

WSO2 Carbon 4.4.X Update 2017-04-03

This update fixes the issue of not deleting old Metrics data in the database by the Metrics Database Cleanup Task.

Bug Fixes

- [CMETRICS-3](#) - Metrics Database Cleanup Task is not deleting old data
-

WSO2 Carbon 4.4.X Update 2017-04-04

This update includes fixes for XSS security vulnerabilities found in carbon admin console.

WSO2 Carbon 4.4.X Update 2017-04-04

This update fixes an issue where under high concurrency, UserStoreConfigXMLProcessor fails to decrypt the connection password in the secondary userstore file.

Bug Fixes

- [IDENTITY-5834](#) - Under high concurrency UserStoreConfigXMLProcessor fails to decrypt the connection password in the secondary userstore file
-

WSO2 Carbon 4.4.X Update 2017-04-06

This will fix a identified security issue.

WSO2 Carbon 4.4.X Update **2017-04-06**

This update fixes a potential Cross Site Scripting (XSS) vulnerability in the ndatasource component of the WSO2 server.

WSO2 Carbon 4.4.X Update **2017-04-07**

This update fixes the issue of failure (on some occasions) in an update and insertOverwrite operation of Siddhi RDBMS event tables.

Bug Fixes

- [ANLYAPIM-150](#) - Error using RDBMS Event Table in siddhi query

WSO2 Carbon 4.4.X Update **2017-04-11**

This update will fix the csrf issue after the tomcat upgrade.

Bug Fixes

- [CEP-1600](#) - Event Simulator UI csrf issue after Tomcat Upgrade

WSO2 Carbon 4.4.X Update **2017-04-11**

This update will fix the issue of returning un-expected results when joining an event stream with a table (which has inconsistency in data) using a window of Length 0.

Bug Fixes

- [SIDDHI-30](#) - Issue in length window (#window.length(0))

WSO2 Carbon 4.4.X Update **2017-04-17**

This update will fix the issue of subtheme not get apply when click the wso2 logo in dashboard due to missing / at the end.

Bug Fixes

- [CDASHBOARD-9](#) - Customize theme doesn't work when no changes in templates/global-navigation.jag

WSO2 Carbon 4.4.X Update **2017-04-17**

This update fixes following security vulnerabilities: - Possible reflected cross-site scripting (XSS) vulnerability in Event Tracer component. - Auto-completion has not being turned off for some of the password fields in 'Create Event Publisher' UI.

WSO2 Carbon 4.4.X Update **2017-04-17**

This update includes fixes for XSS security vulnerabilities found in carbon admin console.

WSO2 Carbon 4.4.X Update **2017-04-18**

This update fixes the issue of 'java.lang.OutOfMemoryError: GC overhead limit exceeded' when starting a product having a JDBC user store with a large user base using -Dsetup option.

Bug Fixes

- [CARBON-16119](#) - OOM error when starting a product with -Dsetup having large user base.
-

WSO2 Carbon 4.4.X Update **2017-04-20**

This update introduces a configurable waiting time for JMS message listeners

Bug Fixes

- [CEP-1603](#) - Event Receiver (Pull mode) consume events before depend artifacts are get deployed

Instructions

```
Add a property as follows,  
<property key="listenerWaitingTimeInMillis">[Time in milliseconds]</property>  
  
to 'jms' adaptorConfig in <CARBON_SERVER>/repository/conf/input-event-adapters.xml. Once the  
configuration is added restart the server.
```

WSO2 Carbon 4.4.X Update **2017-04-21**

This will upgrade the embedded tomcat version to 7.0.77 due to the security vulnerabilities identified in older versions.

WSO2 Carbon 4.4.X Update **2017-04-21**

This update will introduce a method in InputEventAdapterService API to retrieve event subscribers in DAS/CEP.

Bug Fixes

- [CANALYTCOM-15](#) - API to retrieve event subscribers in Event Input Adapter
-

WSO2 Carbon 4.4.X Update **2017-04-24**

This update fixes stack overflow error occurs when processing a message secured with a SAML token with WS-Security.

Bug Fixes

- [IDENTITY-5867](#) - Stack Overflow message occurs when processing a WS-Security message.

WSO2 Carbon 4.4.X Update 2017-04-24

This update fixes possible Hazelcast out of memory issues while clearing the caches.

Bug Fixes

- [CARBON-16093](#) - OOM error while removing map in HazelcastDistributedMapProvider

WSO2 Carbon 4.4.X Update 2017-04-25

This update contain a fix for a regression occurred by update 0956 or patch0956. The NPE is caused when there is no SOAPAction header present on SOAP1.1 service in pass-through proxy.

Bug Fixes

- [IDENTITY-5878](#) - NullPointerException at RampartReceiver

WSO2 Carbon 4.4.X Update 2017-04-28

This update fixes possible Stored Cross Site Scripting (XSS) vulnerability detected in a JavaScript utility used for displaying messages in the Management Console.

WSO2 Carbon 4.4.X Update 2017-04-28

This update fixes possible Stored Cross Site Scripting (XSS) vulnerability detected in a JavaScript utility used for displaying messages in the Management Console.

WSO2 Carbon 4.4.X Update 2017-05-05

This update introduces additional debug logs to print the IP address of the clients connecting to thrift authentication service

Bug Fixes

- [DAS-521](#) - Improvement for identifying the user connected to DAS receiver

Instructions

INSTALLATION INSTRUCTIONS

- (i) Shutdown the server, if it's already started.

```
(ii) Add the following entry to <CARBON_SERVER>/repository/conf/log4j.properties
log4j.logger.org.wso2.carbon.databridge.receiver.thrift=DEBUG

(iii) Restart the server
```

WSO2 Carbon 4.4.X Update 2017-05-07

This update solves potential security issues found in Dashboard portal login-controller.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0260](#)

WSO2 Carbon 4.4.X Update 2017-05-15

DAS server starts receiving data via thrift before the dependent artifacts are deployed (stream definitions, etc.). Thereby, it causes a data loss

Bug Fixes

- [DAS-522](#) - DAS receiver node accepts events before starting the carbon server

Instructions

```
(i) Shutdown the server, if you have already started.

(ii) Add a property to the <dataReceiver name="Thrift"> configuration in the file '<CARBON_SERVER>
/repository/conf/data-bridge/data-bridge-config.xml' as follows,
<config name="waitingTimeInMilliseconds">{waitingTime}</config>

(iii) Restart the server with :
Linux/Unix : sh wso2server.sh
Windows : wso2server.bat
```

WSO2 Carbon 4.4.X Update 2017-05-18

DAS server starts receiving data via thrift before the dependent artifacts are deployed (stream definitions, etc.). Thereby, it causes a data loss

Bug Fixes

- [DAS-522](#) - DAS receiver node accepts events before starting the carbon server

Instructions

```
(i) Shutdown the server, if you have already started.

(ii) Add a property to the <dataReceiver name="Thrift"> configuration in the file '<CARBON_SERVER>
/repository/conf/data-bridge/data-bridge-config.xml' as follows,
<config name="waitingTimeInMilliseconds">{waitingTime}</config>

(iii) Restart the server with :
Linux/Unix : sh wso2server.sh
Windows : wso2server.bat
```

WSO2 Carbon 4.4.X Update 2017-05-19

This update fixes an issue related to DAS 310 SparkJDBC provider, where the spark server hangs when null values are inserted to Oracle database columns which are marked as primary keys.

Bug Fixes

- [DAS-525](#) - Spark Hangs for merge query in Oracle when null value for Composite Primary Key
-

WSO2 Carbon 4.4.X Update **2017-05-19**

This update will remove the warning on OS validation failure.

Bug Fixes

- [CARBON-16125](#) - Remove OS Validating WARNING in 4.4.x
-

WSO2 Carbon 4.4.X Update **2017-05-27**

This update will fix a json parsing issue when retrieving the conf.json file in the gadget generation wizard.

Bug Fixes

- [UES-1133](#) - Gadget is not working as expected due to JSON Parsing error
-

WSO2 Carbon 4.4.X Update **2017-05-27**

In the designer mode of portal application, gadget listing drops one gadget from the gadget store.

Bug Fixes

- [UES-1134](#) - Gadget listing in the designer page drops one gadget
-

WSO2 Carbon 4.4.X Update **2017-05-29**

This update fixes the a race condition that could occur when large number of connections are made to the thrift receiver in a burst.

Bug Fixes

- [DAS-527](#) - Read time out errors getting printed when trying to publish events to DAS receivers
-

WSO2 Carbon 4.4.X Update **2017-05-30**

This update fixes the NPE in axis2json validateArgumentTypes method

Bug Fixes

- [wso2/product-ei#582](#) - NPE when invoking batchrequest with json payload in EI
-

WSO2 Carbon 4.4.X Update 2017-06-03

Encode onOKCallback request parameter to mitigate XSS vulnerability exists in registry browser UI.

WSO2 Carbon 4.4.X Update 2017-06-27

This update will fix a concurrency issue which might lead to events getting dropped at the event publisher component.

Bug Fixes

- [DAS-577](#) - DAS 3.1.0 minimum HA setup fails to persist half of the events
-

WSO2 Carbon 4.4.X Update 2017-06-29

This happens only when the cluster is configured with profiles (analyzers and receivers separately). Let say that the analyzer nodes are started first, then run the spark script. Lets say in spark we create a table called Foo(not the spark temporary table name, this is the actual DAS table). Spark by default creates the tables in processed_data_store. After the table is created, lets say we start the receiver nodes and these receiver nodes have a stream called Foo which is supposed to be persisted. Receiver does not check if the Foo table is already there in any of the recordstores (processed_data_store or event_store). it simply create another Foo table in event_store (which is the default location for persisted stream). Now we have two tables created for the same name in two record stores. Also DAS internal table mapping is changed because of that. So the next time spark runs the script it might refer to the new foo table which is created by the stream persistence. Now that the table mapping is changed and when the DAL is searching for the table, it might throw the following exception saying that it cannot find the specific table. The table is actually there in the table mapping but actually the table is not there in the recordStore. TID: [-1234] [] [2017-06-25 23:01:11,370] ERROR {org.wso2.siddhi.core.query.processor.stream.AbstractStreamProcessor} - Dropping event chunk EventChunk{first=null}, error in processing org.wso2.siddhi.core.query.processor.stream.window.LengthWindowProcessor, Error in getting event records with values: [-1234: ORG_WSO2_ANALYTICS_APIM_REQUESTPERCENTILE] does not exist {org.wso2.siddhi.core.query.processor.stream.AbstractStreamProcessor} java.lang.IllegalStateException: Error in getting event records with values: [-1234:ORG_WSO2_ANALYTICS_APIM_REQUESTPERCENTILE] does not exist at org.wso2.carbon.analytics.eventtable.AnalyticsEventTable\$AnalyticsTableOperator.getRecordWithEventValuesDirect(AnalyticsEventTable.java:837) at org.wso2.carbon.analytics.eventtable.AnalyticsEventTable\$AnalyticsTableOperator.getRecordWithEventValues(AnalyticsEventTable.java:806) at org.wso2.carbon.analytics.eventtable.AnalyticsEventTable\$AnalyticsTableOperator.findRecords(AnalyticsEventTable.java:740) at org.wso2.carbon.analytics.eventtable.AnalyticsEventTable\$AnalyticsTableOperator.find(AnalyticsEventTable.java:722) at org.wso2.carbon.analytics.eventtable.AnalyticsEventTable.find(AnalyticsEventTable.java:295)

Bug Fixes

- [DAS-578](#) - Error in getting event records with values: [-1234: ORG_WSO2_ANALYTICS_APIM_REQUESTPERCENTILE] does not exist
-

WSO2 Carbon 4.4.X Update 2017-07-07

This update fixes XSS vulnerabilities found in the Carbon registry resource UI.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0280](#)

WSO2 Carbon 4.4.X Update 2017-07-10

This update includes fixes for XSS security vulnerabilities found in carbon admin console.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0265](#)

WSO2 Carbon 4.4.X Update 2017-08-04

This update addresses : Indexing data loss during indexernode shutdown issue. The contains() call retrieves actual records from the DB as opposed to checking existence. This could be improved for performance.

Bug Fixes

- [DAS-585](#) - Analytics Event Table contains() retrieves records
 - [DAS-586](#) - Indexing data loss during indexernode shutdown.
-

WSO2 Carbon 4.4.X Update 2017-08-04

This update fix below issues and features, - Siddhi event table update issue when configured with MSSQL database - Inability to configure Siddhi state persistence when clustering is disabled (single node mode) - Failure to load template manager when option fields are configured - MSSQL based persistence store for Siddhi

Bug Fixes

- [DAS-584](#) - Cannot enable Siddhi state persistence when Clustering is disabled (single node mode)
- [DAS-587](#) - RDBMS event table does not work with MSSQL Server.
- [DAS-588](#) - Template manager fails when loading option fields
- [DAS-589](#) - MSSQL based Persistence Store for Siddhi

Instructions

Copy below configuration to <CARBON_SERVER>/repository/conf/event-processor.xml file, under the <eventProcessorConfiguration> tag to enable file persistence for single node mode. Only use below configuration if file based persistence is required for stand alone mode.

```
<mode name="SingleNode" enable="true">
<persistence enable="true">
<persistenceIntervalInMinutes>1</persistenceIntervalInMinutes>
<persisterSchedulerPoolSize>10</persisterSchedulerPoolSize>
<persister class="org.wso2.carbon.event.processor.core.internal.persistence.
FileSystemPersistenceStore">
<property key="persistenceLocation">cep_persistence</property>
</persister>
</persistence>
</mode>
```

WSO2 Carbon 4.4.X Update 2017-08-04

When a proxy invokes a backend which will respond with the soap attachment. In the proxy's out sequence a content aware mediator is there. And when the response received by the client, it will have two attachment. the original attachment from backend and the original payload as another attachment.

Bug Fixes

- [ESBJAVA-5072](#) - Soap part comes as attachment when a content aware mediator is in out sequence
-

WSO2 Carbon 4.4.X Update 2017-08-11

This update alters the maximum limit of the databridge server's worker thread pool size, in order to avoid certain possibilities of server going out of memory. Earlier, maximum size of the thread pool was 2147483647 which is the default value assigned by Apache Thrift library. This update overrides that default value and sets the default max thread pool size to be 20. After this update is applied, the max thread pool size will be configurable too. The update also introduces a few other configurable parameters for databridge server. Those can be configured in `<CARBON_HOME>/repository/conf/data-bridge/data-bridge-config.xml` file. Newly introduced parameters are explained below. All of these parameters are optional. TCP configurations: `tcpMaxWorkerThreads`: The maximum size of the data receiving worker thread pool. Default value is 20. `tcpMinWorkerThreads`: The minimum or the starting size of the data receiving worker thread pool. Default value is 5. `tcpRequestTimeout`: The request timeout in milliseconds. Default value is 20. `tcpStopTimeoutVal`: The stop timeout in milliseconds. Default value is 60. SSL configurations: `sslMaxWorkerThreads`: The maximum size of the authenticating worker thread pool. Default value is 20. `sslMinWorkerThreads`: The minimum or the starting size of the authenticating worker thread pool. Default value is 5. `sslRequestTimeout`: The request timeout in milliseconds. Default value is 20. `sslStopTimeoutVal`: The stop timeout in milliseconds. Default value is 60. A sample configuration is given below: `<dataBridgeConfiguration>
<!-- Please note that other existing configurations are omitted for clarity -->
<dataReceiver
name=Thrift>
<config name=tcpPort>7611</config>
<config name=sslPort>7711</config>
<config name=tcpMaxWorkerThreads>25</config>
<config name=tcpMinWorkerThreads>6</config>
<config name=tcpRequestTimeout>30</config>
<config name=tcpStopTimeoutVal>120</config>
<config name=sslMaxWorkerThreads>25</config>
<config name=sslMinWorkerThreads>6</config>
<config name=sslRequestTimeout>30</config>
<config name=sslStopTimeoutVal>120</config>
</dataReceiver>
Configuring Data Agents: When configuring data agents which publish to databridge server, make sure that the databridge server worker thread pool size is greater than the number of data agent threads publishing to the databridge. This is so the databridge server will be able to manage the concurrent data publishers. Refer [1] on how to set up and configure data publishing agents. The number of data agent threads can be specified in <CARBON_HOME>/repository/conf/data-bridge/data-agent-config.xml configuration file. [1] https://docs.wso2.com/display/DAS310/Publishing+Data+Using+Java+Client+Through+Thrift+or+Binary`

Bug Fixes

- [DAS-590](#) - Databridge queue worker thread max count should be limited
-

WSO2 Carbon 4.4.X Update 2017-08-13

This update fixes carbon styles conflict which happens in shared registry mode..

Bug Fixes

- [CARBON-14740](#) - Improve Carbon UI framework to load UI resources from fragment bundles.
-

WSO2 Carbon 4.4.X Update 2017-08-17

This update solves potential security issues found in Dashboard portal login.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0311](#)

WSO2 Carbon 4.4.X Update 2017-09-01

This update fixes the security vulnerability of dashboard settings page being vulnerable to XSS attacks.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0316](#)

WSO2 Carbon 4.4.X Update 2017-09-07

This update addresses an HTML/JS/XSS injection vulnerability found in Activity Explorer component when viewing activities that match a given search criteria.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0322](#)

WSO2 Carbon 4.4.X Update 2017-09-28

This updates the underlying tomcat version to 7.0.81.

Please note that this is a security update. For more information please view [Security Advisory WSO2-2017-0326](#)

WSO2 Carbon 4.4.X Update 2017-10-02

This update fixes the SSLException thrown when -DhttpClient.hostnameVerifier=<property_value> is set in wso2server.sh.

Bug Fixes

- [ESBJAVA-5233](#) - -DhttpClient.hostnameVerifier=<property_value> not working as expected
-

WSO2 Carbon 4.4.X Update 2017-10-13

Fixes for issues found during the test hackathon.

Bug Fixes

- [wso2/carbon-analytics-common#377](#) - Null pointer issue in data bridge
- [wso2/carbon-analytics#463](#) - NotEqual operation not working in Event tables
- [wso2/siddhi#572](#) - When updating RDBMS event tables, only the first attribute of the table can be given for on condition
- [wso2/siddhi#588](#) - Cron window expire event issue
- [wso2/siddhi#190](#) - Fixed `IS NULL` syntax in RDBMS
- [wso2/siddhi#592](#) - Eventtable insert overwrite dont work other than usual cases
- [wso2/carbon-analytics-common#378](#) - Issue in deleting stream by Id in secure event transmission service
- [wso2/carbon-analytics#462](#) - Event table filter conditions not supporting constants

- [wso2/carbon-analytics#464](#) - CategoryPath is null when creating an AnalyticsDrillDownRequest Object for DrillDownRangeCount method
 - [wso2/carbon-analytics#465](#) - Unsupported TaxonomyWriterCacheType error log is showing
 - [wso2/siddhi#579](#) - Partitions with no executors are allowed in Siddhi Query API
 - [wso2/siddhi#589](#) - Issue in adding event windows within partitions
-

WSO2 Carbon 4.4.X Update **2017-10-18**

This update allows the RDBMS event publisher to publish NULL values to string type data fields in DB table.

Bug Fixes

- [DAS-596](#) - DAS RDBMSEventAdapter throws an error when trying execute spark script

Instructions

```
INSTALLATION INSTRUCTIONS
-----
(i) Shutdown the server, if you have already started.

(ii) Restart the server with :
Linux/Unix : sh wso2server.sh
Windows : wso2server.bat
```

Security Advisories

Security Advisory **WSO2-2017-0260**

Overview

A potential Cross-Site Scripting (XSS) vulnerability is detected in dashboard portal.

Description

This addresses a potential XSS vulnerability identified in dashboard portal login-controller when sso is enabled. It has been identified that two such parameters displayed in the HTML page result were not properly encoded before displaying.

Severity

Medium

Impact

An attacker can include malicious content in a request to the dashboard portal, and trick a user to click a crafted URL via email, IM or a neutral web site. This reflects the attack back to the user's browser and will execute the injected code, which may generate malicious page results that will mislead the victim or harm otherwise.

Solution

The recommended solution is to apply the provided patch/update to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

N/A

Security Advisory **WSO2-2017-0265**

Overview

A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console.

Description

This vulnerability is discovered in the message dialog page of the Management Console. However, exploiting the vulnerability remotely is not possible as the malicious script should be injected to an input and given input should be displayed back to the user in a message dialog box.

Severity

Medium

Impact

By leveraging an XSS attack, an attacker can make the browser get redirected to a malicious website, make changes in the UI of the web page, retrieve information from the browser or harm otherwise.

However, since all the session related sensitive cookies are set with httpOnly flag and protected, session hijacking or similar attack would not be possible.

Solution

The recommended solution is to apply the provided patch/update to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

N/A

Security Advisory **WSO2-2017-0280**

Overview

A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console.

Description

This vulnerability is discovered in the flow of adding a registry resource collection from the Management Console. The operation is done via HTTP POST and therefore, in order to exploit the vulnerability, an attacker would require hosting a malicious website and trick the user to visit the website, which would send a malicious request to WSO2 server.

Severity

Medium

Impact

By leveraging an XSS attack, an attacker can make the browser get redirected to a malicious website, make changes in the UI of the web page, retrieve information from the browser or harm otherwise.

However, since all the session related sensitive cookies are set with httpOnly flag and protected, session hijacking or similar attack would not be possible.

Solution

The recommended solution is to apply the provided patch/update to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

WSO2 thanks, sathish@cybersecurityworks.com of Cyber Security Works Pvt Ltd for responsibly reporting the identified issues and working with us as we addressed them.

Security Advisory **WSO2-2017-0311**

Overview

The Portal application is found to be vulnerable to password brute force attacks.

Description

The Account Recovery and Credential Management feature does not enforce account locking, after reaching the maximum failed login attempts count.

Severity

Low

Impact

By leveraging a password brute force attack vulnerability, an attacker would be able to gain access to the Portal web application and compromise the user account of the victim.

Solution

The recommended solution is to apply the provided patch/update to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

null

Security Advisory **WSO2-2017-0316**

Overview

A potential Stored Cross-Site Scripting (XSS) vulnerability has been identified in Dashboard Portal web application.

Description

The XSS vulnerability is identified in Dashboard Portal application when editing the settings of a dashboard.

Severity

Medium

Impact

This vulnerability can lead to HTML injection attacks, reflects the attack back to the user's browser and will execute the injected code, which may generate malicious page results that will mislead the victim or harm otherwise.

Solution

The recommended solution is to apply the provided patch/update which sanitizes the inputs to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

null

Security Advisory **WSO2-2017-0322**

Overview

A potential HTML/JS/XSS injection vulnerability has been identified in Activity Explorer dashboard component.

Description

The HTML/JS/XSS injection vulnerability is identified in Activity Explorer application when viewing activities that match the search criteria.

Severity

Low

Impact

This vulnerability can lead to HTML injection attacks, reflects the attack back to the user's browser and will execute the injected code, which may generate malicious page results that will mislead the victim or harm otherwise.

Solution

The recommended solution is to apply the provided patch/update which encodes HTML for proper viewing, to the affected versions of the products.

Notes

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

null

Security Advisory **WSO2-2017-0326**

Overview

Upgrade the embedded Apache Tomcat version to 7.0.81 to support Tomcat level security fixes.

Description

Some security vulnerabilities have been identified in Tomcat versions prior to 7.0.81. For more details please refer to https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.81

Severity

Medium

Impact

The WSO2 servers may exposed to known vulnerabilities of Apache Tomcat versions prior to 7.0.81

Solution

The recommended solution is to apply relevant security patches/updates which will upgrade the embedded tomcat version of the products to 7.0.81

Notes

We have already tested these patches/updates in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

If you have any questions regarding this advisory, please post them to security@wso2.com.

Credits

N/A

Updated Files

- org.wso2.carbon.analytics.dataservice.core_1.2.7.jar
- org.wso2.carbon.analytics.eventtable_1.2.7.jar
- repository/components/plugins/axis2-json_1.6.1.wso2v20.jar
- repository/components/plugins/axis2_1.6.1.wso2v20.jar
- repository/components/plugins/commons-httpclient_3.1.0.wso2v3.jar
- repository/components/plugins/org.wso2.carbon.analytics.activitydashboard.ui_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.dataservice.commons_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.dataservice.core_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.datasource.cassandra_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.datasource.rdbms_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.eventsink_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.eventtable_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.analytics.spark.core_1.2.7.jar
- repository/components/plugins/org.wso2.carbon.core.bootup.validator_4.4.9.jar
- repository/components/plugins/org.wso2.carbon.core_4.4.9.jar
- repository/components/plugins/org.wso2.carbon.databridge.agent_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.databridge.commons_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.databridge.core_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.databridge.receiver.thrift_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.input.adapter.core_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.input.adapter.jms_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.input.adapter.kafka_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.output.adapter.jms_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.output.adapter.rdbms_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.processor.core_2.1.4.jar
- repository/components/plugins/org.wso2.carbon.event.processor.manager.core_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.publisher.core_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.publisher.ui_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.receiver.core_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.simulator.ui_2.1.4.jar
- repository/components/plugins/org.wso2.carbon.event.template.manager.ui_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.event.tracer.ui_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.identity.authenticator.saml2.sso.common_5.1.3.jar
- repository/components/plugins/org.wso2.carbon.logging.admin.ui_4.5.4.jar
- repository/components/plugins/org.wso2.carbon.metrics.impl_1.2.2.jar
- repository/components/plugins/org.wso2.carbon.ml.commons_1.2.2.jar
- repository/components/plugins/org.wso2.carbon.ml.database_1.2.2.jar
- repository/components/plugins/org.wso2.carbon.ndatasource.ui_4.5.4.jar
- repository/components/plugins/org.wso2.carbon.registry.common_4.6.0.jar
- repository/components/plugins/org.wso2.carbon.registry.resource.ui_4.6.0.jar
- repository/components/plugins/org.wso2.carbon.registry.search.ui_4.6.0.jar
- repository/components/plugins/org.wso2.carbon.roles.mgt.ui_4.4.9.jar
- repository/components/plugins/org.wso2.carbon.security.mgt.ui_5.2.0.jar

- repository/components/plugins/org.wso2.carbon.tenant.mgt.ui_4.6.0.jar
 - repository/components/plugins/org.wso2.carbon.tenant.mgt_4.6.0.jar
 - repository/components/plugins/org.wso2.carbon.tomcat.patch_4.7.0.jar
 - repository/components/plugins/org.wso2.carbon.tryit_4.5.4.jar
 - repository/components/plugins/org.wso2.carbon.ui_4.4.9.jar
 - repository/components/plugins/org.wso2.carbon.user.core_4.4.9.jar
 - repository/components/plugins/org.wso2.carbon.user.mgt.ui_5.2.0.jar
 - repository/components/plugins/rampart-core_1.6.1.wso2v21.jar
 - repository/components/plugins/siddhi-core_3.1.2.jar
 - repository/components/plugins/siddhi-extension-event-table_3.1.2.jar
 - repository/components/plugins/tomcat-catalina-ha_7.0.70.wso2v1.jar
 - repository/components/plugins/tomcat-el-api_7.0.70.wso2v1.jar
 - repository/components/plugins/tomcat-jsp-api_7.0.70.wso2v1.jar
 - repository/components/plugins/tomcat-servlet-api_7.0.70.wso2v1.jar
 - repository/components/plugins/tomcat_7.0.70.wso2v1.jar
 - repository/components/plugins/wss4j_1.5.11.wso2v14.jar
 - repository/deployment/server/jaggeryapps/portal/extensions/authentication/sso-login.jag
 - repository/deployment/server/jaggeryapps/portal/extensions/providers/rdbms/api.js
 - repository/deployment/server/jaggeryapps/portal/extensions/providers/rdbms/config.json
 - repository/deployment/server/jaggeryapps/portal/js/dashboard-settings.js
 - repository/deployment/server/jaggeryapps/portal/js/designer.js
 - repository/deployment/server/jaggeryapps/portal/modules/constants.js
 - repository/deployment/server/jaggeryapps/portal/modules/user.js
 - repository/deployment/server/jaggeryapps/portal/templates/gadgets/gadget-generation-templates/js/gadget-core.js.hbs
 - repository/deployment/server/jaggeryapps/portal/theme/templates/global-navigation.jag
-

Added Files

- bin/tomcat-juli-7.0.75.jar
 - bin/tomcat-juli-7.0.77.jar
 - bin/tomcat-juli-7.0.81.jar
 - lib/endorsed/tomcat-annotations-api-7.0.75.jar
 - lib/endorsed/tomcat-annotations-api-7.0.77.jar
 - lib/endorsed/tomcat-annotations-api-7.0.81.jar
-

Removed Files

- bin/tomcat-juli-7.0.70.jar
 - bin/tomcat-juli-7.0.75.jar
 - bin/tomcat-juli-7.0.77.jar
 - lib/endorsed/tomcat-annotations-api-7.0.70.jar
 - lib/endorsed/tomcat-annotations-api-7.0.75.jar
 - lib/endorsed/tomcat-annotations-api-7.0.77.jar
-