Update Summary for
wso2is - 5.5.0 1553763843419 (full)

This document contains details of 144 update(s) installed into your wso2is-5.5.0 (full) distribution. There are 23 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 2018-04-25
- WSO2 Carbon 4.4.X Update 2018-05-01
- WSO2 Carbon 4.4.X Update 2018-05-08
- WSO2 Carbon 4.4.X Update 2018-06-19
- WSO2 Carbon 4.4.X Update 2018-06-25
- WSO2 Carbon 4.4.X Update 2018-07-19
- WSO2 Carbon 4.4.X Update 2018-08-08
- WSO2 Carbon 4.4.X Update 2018-08-08
- WSO2 Carbon 4.4.X Update 2018-09-25
- WSO2 Carbon 4.4.X Update 2018-10-25
- WSO2 Carbon 4.4.X Update 2018-11-07
- WSO2 Carbon 4.4.X Update 2018-11-27
- WSO2 Carbon 4.4.X Update 2018-11-28
- WSO2 Carbon 4.4.X Update 2018-12-05
- WSO2 Carbon 4.4.X Update 2018-12-07
- WSO2 Carbon 4.4.X Update 2019-01-08
- WSO2 Carbon 4.4.X Update 2019-02-06
- WSO2 Carbon 4.4.X Update 2019-02-09
- WSO2 Carbon 4.4.X Update 2019-03-07
- WSO2 Carbon 4.4.X Update 2019-03-12
- WSO2 Carbon 4.4.X Update 2019-03-12
- WSO2 Carbon 4.4.X Update 2019-03-19
- WSO2 Carbon 4.4.X Update 2019-03-26

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

- WSO2 Carbon 4.4.X Update 2018-04-25
- WSO2 Carbon 4.4.X Update 2018-06-01
- WSO2 Carbon 4.4.X Update 2018-04-25
- WSO2 Carbon 4.4.X Update 2018-06-04
- WSO2 Carbon 4.4.X Update 2018-06-05
- WSO2 Carbon 4.4.X Update 2018-06-15
- WSO2 Carbon 4.4.X Update 2018-06-25
- WSO2 Carbon 4.4.X Update 2018-07-06
- WSO2 Carbon 4.4.X Update 2018-07-19
- WSO2 Carbon 4.4.X Update 2018-07-23
- WSO2 Carbon 4.4.X Update 2018-08-01
- WSO2 Carbon 4.4.X Update 2018-08-01

- WSO2 Carbon 4.4.X Update 2018-08-01
- WSO2 Carbon 4.4.X Update 2018-08-11
- WSO2 Carbon 4.4.X Update 2018-08-13
- WSO2 Carbon 4.4.X Update 2018-08-20
- WSO2 Carbon 4.4.X Update 2018-08-24
- WSO2 Carbon 4.4.X Update 2018-08-27
- WSO2 Carbon 4.4.X Update 2018-08-27
- WSO2 Carbon 4.4.X Update 2018-08-29
- WSO2 Carbon 4.4.X Update 2018-09-04
- WSO2 Carbon 4.4.X Update 2018-09-04
- WSO2 Carbon 4.4.X Update 2018-09-04
- WSO2 Carbon 4.4.X Update 2018-09-07
- WSO2 Carbon 4.4.X Update 2018-09-08
- WSO2 Carbon 4.4.X Update 2018-09-11
- WSO2 Carbon 4.4.X Update 2018-09-25
- WSO2 Carbon 4.4.X Update 2018-09-25
- WSO2 Carbon 4.4.X Update 2018-09-28
- WSO2 Carbon 4.4.X Update 2018-10-08
- WSO2 Carbon 4.4.X Update 2018-10-08
- WSO2 Carbon 4.4.X Update 2018-10-11
- WSO2 Carbon 4.4.X Update 2018-10-13
- WSO2 Carbon 4.4.X Update 2018-10-16
- WSO2 Carbon 4.4.X Update 2018-10-18
- WSO2 Carbon 4.4.X Update 2018-10-25
- WSO2 Carbon 4.4.X Update 2018-11-05
- WSO2 Carbon 4.4.X Update 2018-11-07
- WSO2 Carbon 4.4.X Update 2018-11-07
- WSO2 Carbon 4.4.X Update 2018-11-26
- WSO2 Carbon 4.4.X Update 2018-11-26
- WSO2 Carbon 4.4.X Update 2018-11-26
- WSO2 Carbon 4.4.X Update 2018-11-27
- WSO2 Carbon 4.4.X Update 2018-11-27
- WSO2 Carbon 4.4.X Update 2018-11-27
- WSO2 Carbon 4.4.X Update 2018-11-28
- WSO2 Carbon 4.4.X Update 2018-11-28
- WSO2 Carbon 4.4.X Update 2018-12-05
- WSO2 Carbon 4.4.X Update 2018-12-07
- WSO2 Carbon 4.4.X Update 2018-12-14
- WSO2 Carbon 4.4.X Update 2019-01-08
- WSO2 Carbon 4.4.X Update 2019-01-08
- WSO2 Carbon 4.4.X Update 2019-01-16
- WSO2 Carbon 4.4.X Update 2019-01-29
- WSO2 Carbon 4.4.X Update 2019-01-29
- WSO2 Carbon 4.4.X Update 2019-02-02
- WSO2 Carbon 4.4.X Update 2019-02-09
- WSO2 Carbon 4.4.X Update 2019-02-27
- WSO2 Carbon 4.4.X Update 2019-03-12
- WSO2 Carbon 4.4.X Update 2019-03-24
- WSO2 Carbon 4.4.X Update 2019-03-26
- WSO2 Carbon 4.4.X Update 2019-03-28

WSO2 Carbon 4.4.X Update 2018-03-22

This update will fix the issue where OIDC Logout call results in a NoClassDefFoundError error.

Bug Fixes

- wso2/product-is#2982 - OIDC Logout call results in a NoClassDefFoundError error.

WSO2 Carbon 4.4.X Update 2018-04-08

Requested claims in are available at the first request but consequent second request to the IS without login out(When the cookie is available) will not return the requested claims.

Bug Fixes

- wso2/carbon-identity-framework#1494 - Requested claims are missing if cookie presents in the OIDC request

---

WSO2 Carbon 4.4.X Update 2018-04-10

When a user tries to login to the application using LDAP userstore and if it fails (invalid credentials), There are two authentication request sent to LDAP (user bind), which ultimately reduce the number allowed re-attempts in LDAP server by 2x.

Bug Fixes

- wso2/carbon-kernel#1738 - Users are being Authenticated against secondary user store twice causing early locking

---

WSO2 Carbon 4.4.X Update 2018-04-16

XACML Multi-decision profile is not working with JSON requests
For enable/disable the shorten-form of JSON, add the property to entitlement.properties file in <carbon-home>/repository/conf/identity/

#Enable JSON shorten form support by default
JSON.Shorten.Form.Enabled=false

Bug Fixes

- wso2/product-is#2999 - XACML Multi-decision profile is not working with JSON requests

---

WSO2 Carbon 4.4.X Update 2018-04-25

While doing user management tasks, audit logs are missing for some important tasks. This update adds additional audit logs for user management activities.

Bug Fixes

- wso2/product-is#2975 - Improve audit logs related with User Management

Instructions

```
Improved audit loggers are disabled by default. Please refer the documentation at https://docs.wso2.
com/display/IS550/Using+the+User+Management+Errors+Event+Listener to enable the audit loggers in
your environment.
```

WSO2 Carbon 4.4.X Update 2018-04-25

When performing bulk user import, have to look through the logs to figure out which ones errored out and there is no separate error file or log file unique to this bulk import that can be used.

Bug Fixes

- wso2/product-is#2892 - Bulk User import improvements.

Instructions

```
With this update you can move bulk user import logs into a separate log file. Please follow the
instructions below.

1. Open <CARBON_HOME>/repository/conf/log4j.properties file.
2. Add the following log4j configuration and save the file.

# Bulk user import log appender.
log4j.logger.org.wso2.carbon.user.mgt.bulkimport=INFO, CARBON_BULK_USER_IMPORT

log4j.appender.CARBON_BULK_USER_IMPORT=org.wso2.carbon.user.mgt.bulkimport.BulkUserImportLogAppender
log4j.appender.CARBON_BULK_USER_IMPORT.File=${carbon.home}/repository/logs/${instance.log}
/bulkuserimport${instance.log}.log
log4j.appender.CARBON_BULK_USER_IMPORT.Append=false
log4j.appender.CARBON_BULK_USER_IMPORT.layout=org.wso2.carbon.utils.logging.TenantAwarePatternLayout
log4j.appender.CARBON_BULK_USER_IMPORT.layout.ConversionPattern=[%T][%d] %P%5p {%c} - %x %m%n
log4j.appender.CARBON_BULK_USER_IMPORT.layout.TenantPattern=%U%@%D [%T] [%S]
log4j.appender.CARBON_BULK_USER_IMPORT.threshold=INFO

3. Restart the server.
```

WSO2 Carbon 4.4.X Update 2018-04-25

Fixing geronimo-kernal by upgrading to 3.0.1 and wso2-axis2 fork
(i) After geting the WUM update. Open the axis2.xml file in <carbon-home>/repository/conf/axis2/ folder (ii) Change the line <messageBuilder contentType="application/xml" class="org.apache.axis2.builder.ApplicationXMLBuilder"/> to <messageBuilder contentType="application/xml" class="org.apache.axis2.builder.SecureApplicationXMLBuilder"/> (iii) Restart the server.

WSO2 Carbon 4.4.X Update 2018-04-25

No error messages display when reusing the redirection URL and when using the redirection URL after the expiry time.

Bug Fixes

- wso2/carbon-identity-framework#1518 - No error messages display when reusing the redirection URL and when using the redirection URL after the expiry time.

WSO2 Carbon 4.4.X Update 2018-05-01

At JIT provisioning, IdP roles mapped for local roles get persisted as a claim in user store. This update fixes persisting roles as a claim.

Bug Fixes

- wso2/product-is#3098 - Cannot provision user with roles when many roles assigned to the user

---

WSO2 Carbon 4.4.X Update 2018-05-01

This update introduces new pattersn to forget me tool to support anonymization of newly introduced user management audit logs

Bug Fixes

- wso2/identity-anonymization-tool#81 - Improve anonymization patterns to anonymize user management audit logs

---

WSO2 Carbon 4.4.X Update 2018-05-01

This fixes the issue of not encoding the 'mediaType' parameter in /carbon/resources /custom_add_ajaxprocessor.jsp and 'path' parameter in /carbon/resources/resource.jsp

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0422

WSO2 Carbon 4.4.X Update 2018-05-03

Seems Office 365 authenticator updated to new version 1.0.4 and SMS-OTP updated to new version 2.0.12 , but these was not shipped with IS 5.5.0.

Bug Fixes

- wso2/product-is#3045 - Connector versions are not updated in IS 5.5.0.

WSO2 Carbon 4.4.X Update 2018-05-08

Stored XSS vulnerability in Add User Store page description field.

Please note that this is a security update. For more information please view Security Advisory WSO2-2017-0197

WSO2 Carbon 4.4.X Update 2018-05-09

Mobile and Device Friendly Support for Identity Server Dashboard

Bug Fixes

- wso2/product-is#3141 - Mobile and Device Friendly Support for Identity Server Dashboard

---

WSO2 Carbon 4.4.X Update 2018-05-09

This update improves OIDC federated authenticator supporting client authentication over HTTP basic authentication scheme

Bug Fixes

- wso2/product-is#3138 - OIDC federated authenticator does not support Basic client authentication

---

WSO2 Carbon 4.4.X Update 2018-05-15

This update fixes a regression issue caused by applying HTML encoding for user store configuration properties while adding user stores from the management console..

Bug Fixes

- wso2/product-is#3072 - WUM Update breaks the secondary user-store by adding a additional "amp;" into GroupNameSearchFilter and UserNameSearchFilter properties.

WSO2 Carbon 4.4.X Update 2018-05-16

This update contains the fix of not having kid value in self contained access token header.

Bug Fixes

- wso2/product-is#3123 - Self Contained Access token does not contain the kid value.

WSO2 Carbon 4.4.X Update 2018-05-17

This update contains fixes for invalid data provided exception when confirming user with UserStoreBasedIdentityDataStore in self user registration flow.

Bug Fixes

- wso2/carbon-identity-framework#1568 - Invalid data provided exception when confirming user with UserStoreBasedIdentityDataStore

---

WSO2 Carbon 4.4.X Update 2018-05-28

This issue is fixed in this update by adding the message id of incoming message context to the newly created message context within LocalTransportReceiver

Bug Fixes

- wso2/product-ei#2173 - Local Transport is Blocking in Aggregation

WSO2 Carbon 4.4.X Update 2018-05-29

Avoid possible null pointer exception in oauth endpoint

Bug Fixes

- wso2/product-is#3231 - Avoid possible null pointer exception in oauth endpoint

WSO2 Carbon 4.4.X Update 2018-05-30

This fixes the issue of not having imports in custom_add_ajaxprocessor.jsp

Bug Fixes

- wso2/product-ei#2196 - Missing imports in JSPs of org.wso2.carbon.registry.resource.ui

WSO2 Carbon 4.4.X Update 2018-06-01

This update fixes the error while SSO consent management in federated scenarios when the username is in email format

Bug Fixes

- wso2/product-is#3079 - Error while SSO consent management in federated scenarios when the username is in email format.

WSO2 Carbon 4.4.X Update 2018-06-01

Certificate Revocation Validation with CRL and OCSP for X509 Authenticator

Bug Fixes

- wso2/product-is#3178 - Certificate Revocation Validation with CRL and OCSP for X509 Authenticator

Instructions

```
This update will add certificate-validation.xml file into CARBON_HOME/repository/conf/security
folder. This is used to configure validators for X509 certificate revocation validation. In there,
when the CRLValidator or OCSPValidator is enabled via <Validator> configuration, in X509
authentication with X509 authenticator, the user certificate will be validated against CRL/OCSP to
verify the certificate revocation.
Please refer WSO2 official documentation for further information.

This update will copy x509certificateauthenticationendpoint.war file into CARBON_HOME/repository
/deployment/server/webapps/ folder. If the x509certificateauthenticationendpoint web application is
customized, get the updated war file, extract it and then get the changes merged with the
customized web application.
If not, get the update and remove the x509certificateauthenticationendpoint directory at CARBON_HOME
/repository/deployment/server/webapps/ path, before starting the server, so that the updated war
file will get deployed.
```

WSO2 Carbon 4.4.X Update 2018-06-04

This update fixes the issue which custom claims coming in JWT assertion are not send with the self contained access token. Further with this update, self conatined access token will include scope and also the expiry time of token will be decided based on the expiry time of incoming assertion.

Bug Fixes

- wso2/product-is#3183 - JWT Grant Type - Custom claims are not stored & not available in the token response and scope sould be part of self contained access token and the expiry time should be decided based on incoming assertion

Instructions

```
Custom claims will be handled only if token request is generated with the scope “openid”.

When “ConvertOriginalClaimsFromAssertionsToOIDCDialect” element under “OpeIDConnect” element in
<Carbon_Home>/repository/conf/identity/identity.xml is set as false as follow,
<OpenIDConnect>
…
<ConvertOriginalClaimsFromAssertionsToOIDCDialect>false<
/ConvertOriginalClaimsFromAssertionsToOIDCDialect>
…
</OpenIDConnect>
All custom claims coming with incoming JWT assertion, will be directly copied to the self contained
access token.

When “ConvertOriginalClaimsFromAssertionsToOIDCDialect” element is set to true, claims will be
handled in the default OIDC flow, incoming claims will be converted to OIDC dialect based on SP and
IDP level claim mappings, and based on claims configured in oidc registry path as mentioned in [1],
only the claims that are specified in relevant openid scope will be copied to the self contained
access token. To copy the attributes that does not have a mapping,”AddUnmappedUserAttributes”
element should be added as follow under “OpeIDConnect” element in <Carbon_Home>/repository/conf
/identity/identity.xml.
<OpenIDConnect>
…
<ConvertOriginalClaimsFromAssertionsToOIDCDialect>true<
/ConvertOriginalClaimsFromAssertionsToOIDCDialect>
<AddUnmappedUserAttributes>true</AddUnmappedUserAttributes>
…
</OpenIDConnect>

“ConvertOriginalClaimsFromAssertionsToOIDCDialect” and “AddUnmappedUserAttributes” elements are
considered to be false by default.

[1] https://docs.wso2.com/display/IS550/Configuring+Claims+for+a+Service+Provider
```

WSO2 Carbon 4.4.X Update 2018-06-05

This update introduces the new crypto service, which is an extensible framework for cryptography in WSO2 servers.

Bug Fixes

- wso2/carbon-kernel#1789 - Use carbon-crypto-service to configure a separate keystore for internal data encryption.

Instructions

```
Currently the key store configured in <Security>/<KeyStore> element in CARBON_HOME/repository/conf
/carbon.xml
is used for internal data encryption as well as for message signing, decryption when communicating
external parties.
```

```
This update allows a separate keystore to be used for internal data encryption.
This feature is provided by the newly introduced Carbon Crypto Service.
It is an extensible framework which facilitates the cryptography needs of Carbon products.

WARNING :
Using a totally new keystore for internal data encryption in an existing deployment will make
already encrypted stored data unusable.
In such cases an appropriate data migration effort is needed.

A common use case of this feature for an existing deployment is,
configuring the existing keystore as the internal keystore for internal data encryption and
using a new keystore when communicating with external parties such SAML, OIDC id_token signing.

In order to use a separate keystore for internal data encryption ...

1) Enable the Crypto Service by adding following configuration block to CARBON_HOME/repository/conf
/carbon.xml

<CryptoService>
<Enabled>true</Enabled>
<InternalCryptoProviderClassName>org.wso2.carbon.crypto.provider.
KeyStoreBasedInternalCryptoProvider</InternalCryptoProviderClassName>
<ExternalCryptoProviderClassName>org.wso2.carbon.core.encryption.
KeyStoreBasedExternalCryptoProvider</ExternalCryptoProviderClassName>
<KeyResolvers>
<KeyResolver className="org.wso2.carbon.crypto.defaultProvider.resolver.
ContextIndependentKeyResolver" priority="-1"/>
</KeyResolvers>
</CryptoService>

2) Configure the new keystore by adding the following configuration block inside the <Security> tag
in CARBON_HOME/repository/conf/carbon.xml

NOTE: The values of the properties such as passwords, should be changed based on the keystore.

<InternalKeyStore>
<Location>${carbon.home}/repository/resources/security/internal.jks</Location>
<Type>JKS</Type>
<Password>wso2carbon</Password>
<KeyAlias>wso2carbon</KeyAlias>
<KeyPassword>wso2carbon</KeyPassword>
</InternalKeyStore>
```

WSO2 Carbon 4.4.X Update 2018-06-05

The filter by role name to return SCIM ID for the Service provider roles (created during the Service Provider creations).

Bug Fixes

- wso2/product-is#3243 - Support SCIM ID generation for groups added via Management Console.

WSO2 Carbon 4.4.X Update 2018-06-05

This update fixes NPE gives in a SAML logout for a tenant scenario when the tenant domain is appended to issuer.

Bug Fixes

- wso2/product-is#3183 - SAML logout gives a NPE for a tenant scenario when the tenant domain is appended to issuer

WSO2 Carbon 4.4.X Update 2018-06-13

This update fix client ID extraction issue during logout when ID Token contains aud claim with multiple values

Bug Fixes

- wso2/product-is#3280 - OidC Session Management RP-initiated logout fails when multiple audience added to id token

---

WSO2 Carbon 4.4.X Update 2018-06-15

Currently in IS the token generation configuration is at the server level configuration which can be configured in the identity.xml. This update provides ability to configur token issuer at the service provider configuration level at the management console

Bug Fixes

- wso2/product-is#3265 - Token generator configuration on consumer level

Instructions

```
This update provides ability to configur token issuer at the service provider configuration level
at the management console. In order to do that you need to register the token issuers
used in IS to the identity.xml as in the following format. First you need to uncomment
<SupportedTokenTypes> element and add the token issuers in the following format inder the
<SupportedTokenTypes>
element.

<SupportedTokenTypes>
......
<SupportedTokenType>
<TokenTypeName>JWT</TokenTypeName>
<TokenTypeImplClass>org.wso2.carbon.identity.oauth2.token.JWTTokenIssuer</TokenTypeImplClass>
<PersistAccessTokenAlias>true</PersistAccessTokenAlias>
</SupportedTokenType>
......
</SupportedTokenTypes>

Following are the parameter definitions

TokenTypeName - unique identifier for the token type
TokenTypeImplClass - token issuer implementation class
PersistAccessTokenAlias - whether to persist the access token alias in the db

If the above configuration is not enabled then the default token issuers which are UUID and JWT
token issuers will be there in the IS.
```

WSO2 Carbon 4.4.X Update 2018-06-19

This update prevents users from uploading malicious zip files via the gadget upload feature in the dashboard.

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0447

WSO2 Carbon 4.4.X Update 2018-06-22

This update will enable sending OIDC claims with a "." in the claim URI. (Ex: org.division)

Bug Fixes

- wso2/product-is#3313 - Claims not retrieved in the IDtoken when having a "." in the claim URI in oidc claim dialect

---

WSO2 Carbon 4.4.X Update 2018-06-25

This update is to avoid malicious archive file upload

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0447

WSO2 Carbon 4.4.X Update 2018-06-25

This update introduces the ability to rename the username of a user, via an API.
This feature has been implemented as an extension to the ForgetMe tool.

Bug Fixes

- wso2/identity-anonymization-tool#84 - Implement an extension to rename username

Instructions

```
Description
===========

- This extension for the forget-me tool, allows the username to be changed.

- OOTB support is available for JDBC and LDAP user stores.

- Can be extended to to support other user store types.

Prerequisites
=============

Since the tool runs outside WSO2 products, it has following limitations.

1) It can't read the encrypted property values in the user store configuration files in the WSO2
product. (e.g. use-mgt.xml)

2) It can't connect to the embedded H2 database, if the WSO2 product has started the H2 database in
non service mode.

Therefore, as a workaround the following steps should be followed before using this extension.

I) Use plaintext in user store configurations.

If it is not an option, the following alternative can be followed.

i) Take a copy of the original config and make them plain text.

The the configurations should be in a folder hierarchy as the original file.

e.g. /wso2/plain-text-configs
- repository
- conf
- user-mgt.xml
- datasources
- master-datasource.xml

ii) Point the extension to use these copies of the product configurations.

(The extension configuration is located in PRODUCT_HOME/repository/components/tools/forget-me/ext
/user-store/conf/)

e.g.
```

```
{
"dir": "/wso2/plain-text-configs",
"type": "user-store",
"processor" : "user-store",
.
.
.
}


II) Configure the WSO2 product to start embedded H2 database in server mode.

AUTO_SERVER=TRUE property in the connection string makes the H2 database to run in server mode.

e.g. jdbc:h2:./repository/database/WSO2CARBON_DB;DB_CLOSE_ON_EXIT=FALSE;LOCK_TIMEOUT=60000;
AUTO_SERVER=TRUE

Extension points
================

As mentioned above the OOTB configuration is sufficient to deal with the default JDBC user store
and LDAP user stores.

In case of extending the feature the following configurations / extension points are available.

(The extension configuration is located in PRODUCT_HOME/repository/components/tools/forget-me/ext
/user-store/conf/)

1) Map a user store handler with a user store manager class name.

{
"dir": "../../../../../../../../",
"type": "user-store",
"processor" : "user-store",
"properties" : [
{
"handler-mapping;org.wso2.carbon.user.core.ldap.CustomActiveDirectoryUserStoreManager":"read-write-
ldap-handler"
}
]
}

2) Change the SQL query for the OOTB JDBC user store handler.

{
"dir": "../../../../../../../../",
"type": "user-store",
"processor" : "user-store",
"properties" : [
{
"handler-property;jdbc-handler;rename.query":"UPDATE MY_USERS SET USERNAME=? WHERE USERNAME=? AND
TENANT_ID=? "
}
]
}

3) Writing a new user store handler and map it with a user store manager class.

- Extend org.wso2.carbon.privacy.forgetme.userstore.handler.UserStoreHandler.

- Implement getName() to return a unique name for the handler. e.g. 'file-based-handler'

- Register the handler with a user store manager class name.

{
"dir": "../../../../../../../../",
"type": "user-store",
"processor" : "user-store",
"properties" : [
{
"handler-mapping;com.xyz.FileBasedUserStoreManager":"file-based-handler"
}
]
}

- If needed properties can be passed to the handler via the configurations.

{
"dir": "../../../../../../../../",
"type": "user-store",
"processor" : "user-store",
"properties" : [
{
"handler-mapping;com.xyz.FileBasedUserStoreManager":"file-based-handler",
"handler-property;file-based-handler;property1":"value1"
```

```
}
]
}

ReST API
========

Request
-------

curl -X PUT \
https://localhost:9443/forgetme/v1.0/user/{tenantId}/{tenantDomain}/{userStoreDomain}/{userName} \
-H 'content-type: application/json' \
-d '{
"username":"{newUserName}"
}'

Response
--------

- Success

HTTP 200

{
"user": {
"username": "<newUserName>"
}
}

- Error

HTTP 500

{
"error": "An error occurred while renaming the user."
}
```

WSO2 Carbon 4.4.X Update 2018-06-28

With the introspection call, one can request user claims with "required_claims" parameter. If JWT token generation is enabled from identity.xml, a JWT with required claims will be returned with the introspection response as additional property "token_string"

Bug Fixes

- wso2/product-is#3327 - Include option to retrieve a JWT with introspection call

WSO2 Carbon 4.4.X Update 2018-06-28

When required configurations are done for setting SCIM2 extension attributes, the "adminForcedPasswordReset" claim does get updated with a PATCH request, but the OTP doesn't gets generated when invoked through SCIM2 api. This update provides a fix for this issue.

Bug Fixes

- wso2/product-is#3320 - OTP Not generated when "adminForcedPasswordReset" claim set through scim2 API

WSO2 Carbon 4.4.X Update 2018-06-29

This update will fix issue by checking the database stores identifiers and then get the tables with correct identifier format.

Bug Fixes

- wso2/carbon-identity-framework#1641 - Uppercase table identifiers are not working for PostgreSQL in DatabaseMetaData#getTables method

WSO2 Carbon 4.4.X Update 2018-07-05

When a federated user account is associated with a local user in a secondary user store, and "Assert identity using mapped local subject identifier" is enabled, in IDN_OAUTH2_ACCESS_TOKEN table should save entries in following format. AUTHZ_USER = <local_username> USER_DOMAIN = <Secondary-Domain>

Bug Fixes

- wso2/product-is#3344 - Add correct User Store Domain details when creating associated local user object in during Post Authentication

WSO2 Carbon 4.4.X Update 2018-07-06

eIDAS profile support for IS

Bug Fixes

- wso2/product-is#3200 - eIDAS profile support for IS

Instructions

```
Please use following database scripts to add SP_CLAIM_DIALECT table to an existing database and
restart the server.

******** H2 ********
CREATE TABLE IF NOT EXISTS SP_CLAIM_DIALECT (
ID INTEGER NOT NULL AUTO_INCREMENT,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID));
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE;


******** MySQL ********
CREATE TABLE IF NOT EXISTS SP_CLAIM_DIALECT (
ID INTEGER NOT NULL AUTO_INCREMENT,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID));
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE;


******** DB2 ********
CREATE TABLE IF NOT EXISTS SP_CLAIM_DIALECT (
ID INTEGER NOT NULL,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID))
/
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE
/
```

```
******** MSSQL ********
IF NOT EXISTS (SELECT * FROM SYS.OBJECTS WHERE OBJECT_ID = OBJECT_ID(N'[DBO].[SP_CLAIM_DIALECT]')
AND TYPE IN (N'U'))
CREATE TABLE SP_CLAIM_DIALECT (
ID INTEGER NOT NULL IDENTITY,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID),
CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID) REFERENCES SP_APP (ID) ON DELETE CASCADE
);


******** Oracle ********
CREATE TABLE SP_CLAIM_DIALECT (
ID INTEGER,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID))
/
CREATE SEQUENCE SP_CLAIM_DIALECT_SEQ START WITH 1 INCREMENT BY 1 NOCACHE
/
CREATE OR REPLACE TRIGGER SP_CLAIM_DIALECT_SEQ
BEFORE INSERT
ON SP_CLAIM_DIALECT
REFERENCING NEW AS NEW
FOR EACH ROW
BEGIN
SELECT SP_CLAIM_DIALECT_SEQ.nextval INTO :NEW.ID FROM dual;
END;
/
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE
/


******** Oracle rac ********
CREATE TABLE SP_CLAIM_DIALECT (
ID INTEGER,
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID))
/
CREATE SEQUENCE SP_CLAIM_DIALECT_SEQ START WITH 1 INCREMENT BY 1 CACHE 20 ORDER
/
CREATE OR REPLACE TRIGGER SP_CLAIM_DIALECT_SEQ
BEFORE INSERT
ON SP_CLAIM_DIALECT
REFERENCING NEW AS NEW
FOR EACH ROW
BEGIN
SELECT SP_CLAIM_DIALECT_SEQ.nextval INTO :NEW.ID FROM dual;
END;
/
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE
/


******** PostgreSQL ********
DROP TABLE IF EXISTS SP_CLAIM_DIALECT;
DROP SEQUENCE IF EXISTS SP_CLAIM_DIALECT_SEQ;
CREATE SEQUENCE SP_CLAIM_DIALECT_SEQ;
CREATE TABLE SP_CLAIM_DIALECT (
ID INTEGER DEFAULT NEXTVAL('SP_CLAIM_DIALECT_SEQ'),
TENANT_ID INTEGER NOT NULL,
SP_DIALECT VARCHAR (512) NOT NULL,
APP_ID INTEGER NOT NULL,
PRIMARY KEY (ID));
ALTER TABLE SP_CLAIM_DIALECT ADD CONSTRAINT DIALECTID_APPID_CONSTRAINT FOREIGN KEY (APP_ID)
REFERENCES SP_APP (ID) ON DELETE CASCADE;






Please use ClaimMetadataManagementService to add following claim dialects and external claims
related to eIDAS attribute profile.

<Dialect dialectURI="http://eidas.europa.eu/attributes/naturalperson">
<Claim>
```

```
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier</ClaimURI>
<DisplayName>Person Identifier</DisplayName>
<AttributeID>scimId</AttributeID>
<Description>Person Identifier</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/userid</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName</ClaimURI>
<DisplayName>Current Family Name</DisplayName>
<AttributeID>sn</AttributeID>
<Description>Current Family Name</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/lastname</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName</ClaimURI>
<DisplayName>Current Given Name</DisplayName>
<AttributeID>givenName</AttributeID>
<Description>Current Given Name</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/givenname</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/DateOfBirth</ClaimURI>
<DisplayName>Date of birth</DisplayName>
<AttributeID>dateOfBirth</AttributeID>
<Description>Date of birth</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/dob</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/BirthName</ClaimURI>
<DisplayName>Birth Name</DisplayName>
<AttributeID>uid</AttributeID>
<Description>Birth Name</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/username</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth</ClaimURI>
<DisplayName>Place of Birth</DisplayName>
<AttributeID>country</AttributeID>
<Description>Place of Birth</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/country</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/CurrentAddress</ClaimURI>
<DisplayName>Current Address</DisplayName>
<AttributeID>localityAddress</AttributeID>
<Description>Current Address</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/addresses</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/Gender</ClaimURI>
<DisplayName>Gender</DisplayName>
<AttributeID>gender</AttributeID>
<Description>Gender</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/gender</MappedLocalClaim>
</Claim>
</Dialect>
<Dialect dialectURI="http://eidas.europa.eu/attributes/legalperson">
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier</ClaimURI>
<DisplayName>Legal Person Identifier</DisplayName>
<AttributeID>externalId</AttributeID>
```

```
<Description>Legal Person Identifier</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/externalid</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/LegalName</ClaimURI>
<DisplayName>Legal Person Name</DisplayName>
<AttributeID>organizationName</AttributeID>
<Description>Legal Person Name</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/organization</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress</ClaimURI>
<DisplayName>Legal Person Address</DisplayName>
<AttributeID>localityAddress</AttributeID>
<Description>Legal Person Address</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/addresses</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber</ClaimURI>
<DisplayName>VAT Registration Number</DisplayName>
<AttributeID>im</AttributeID>
<Description>VAT Registration Number</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/im</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/TaxReference</ClaimURI>
<DisplayName>Tax Reference</DisplayName>
<AttributeID>postalcode</AttributeID>
<Description>Tax Reference</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/postalcode</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/D-2012-17-EUIdentifier</ClaimURI>
<DisplayName>EU Identifier</DisplayName>
<AttributeID>region</AttributeID>
<Description>EU Identifier</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/region</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/LEI</ClaimURI>
<DisplayName>LEI</DisplayName>
<AttributeID>stateorprovince</AttributeID>
<Description>LEI</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/stateorprovince</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/EORI</ClaimURI>
<DisplayName>Economic Operator Registration and Identification</DisplayName>
<AttributeID>departmentNumber</AttributeID>
<Description>Economic Operator Registration and Identification</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/department</MappedLocalClaim>
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/SEED</ClaimURI>
<DisplayName>System for Exchange of Excise Data Identifier</DisplayName>
<AttributeID>nickName</AttributeID>
<Description>System for Exchange of Excise Data Identifier</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/nickname</MappedLocalClaim>
```

```
</Claim>
<Claim>
<ClaimURI>http://eidas.europa.eu/attributes/legalperson/SIC</ClaimURI>
<DisplayName>Standard Industrial Classification</DisplayName>
<AttributeID>formattedName</AttributeID>
<Description>Standard Industrial Classification</Description>
<Required />
<DisplayOrder>1</DisplayOrder>
<SupportedByDefault />
<MappedLocalClaim>http://wso2.org/claims/formattedName</MappedLocalClaim>
</Claim>
</Dialect>


Sample SOAP requests would be as follows:

**** Add Claim Dialect ****
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://org.
apache.axis2/xsd" xmlns:xsd1="http://dto.mgt.metadata.claim.identity.carbon.wso2.org/xsd">
<soapenv:Header/>
<soapenv:Body>
<xsd:addClaimDialect>
<xsd:claimDialect>
<xsd1:claimDialectURI>http://eidas.europa.eu/attributes/naturalperson</xsd1:claimDialectURI>
</xsd:claimDialect>
</xsd:addClaimDialect>
</soapenv:Body>
</soapenv:Envelope>

**** Add External Claim ****
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://org.
apache.axis2/xsd" xmlns:xsd1="http://dto.mgt.metadata.claim.identity.carbon.wso2.org/xsd">
<soapenv:Header/>
<soapenv:Body>
<xsd:addExternalClaim>
<xsd:externalClaim>
<xsd1:externalClaimDialectURI>http://eidas.europa.eu/attributes/naturalperson</xsd1:
externalClaimDialectURI>
<xsd1:externalClaimURI>http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier</xsd1:
externalClaimURI>
<xsd1:mappedLocalClaimURI>http://wso2.org/claims/userid</xsd1:mappedLocalClaimURI>
</xsd:externalClaim>
</xsd:addExternalClaim>
</soapenv:Body>
</soapenv:Envelope>




Please refer [1] for more information on eIDAS profile support in IS.

[1] https://docs.wso2.com/display/IS550
/eIDAS+SAML+Attribute+Profile+Support+via+WSO2+Identity+Server
```

WSO2 Carbon 4.4.X Update 2018-07-08

Fix re-captcha for prompt for SSO flows.

Bug Fixes

- wso2/product-is#3351 - Fix issue on re-captcha prompt for secondary user store users.

WSO2 Carbon 4.4.X Update 2018-07-12

This update provides the ability to change the SP application ownership.

Bug Fixes

- wso2/product-is#3353 - Provide the ability to change the SP ownership

WSO2 Carbon 4.4.X Update 2018-07-17

We only have role based scope validation in token validation step. If scope validator is configured in the application, validation should happen during token generation as well.

Bug Fixes

- wso2/product-is#3354 - Validate scopes against user roles during token generation

WSO2 Carbon 4.4.X Update 2018-07-19

This update contains the fix to not showing "user not found" error during password reset flow.

Instructions

```
This update disables showing "user not found" error during password reset for invalid users by
default.
Add the following property under <Recovery> tag in <Server_Home>/repository/conf/identity/identity.
xml file to enable this.

<NotifyUserExistence>true</NotifyUserExistence>
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0455

WSO2 Carbon 4.4.X Update 2018-07-23

This could be implemented with DCR endpoint. We mandate the client_name parameter for dynamic client registration. This client_name is used as SP name in IS. We can use DCR to get oauth client details using client_name.

Bug Fixes

- wso2/product-is#3446 - Provide REST API to retrieve oauth client data with SP name

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-07-23

This update fixes the issue in Application roles creation and filtering through SCIM.

Bug Fixes

- wso2/product-is#3431 - Issue while creating and filtering Application roles through SCIM

WSO2 Carbon 4.4.X Update 2018-07-23

This update provides capability to have multiple certificates for an identity provider for saml

Bug Fixes

- wso2/product-is#329 - Allow two certificate for a identity provider

---

WSO2 Carbon 4.4.X Update 2018-07-24

This update adds the missing CertificateInfo array element in identity application mgt wsdl

Bug Fixes

- wso2/carbon-identity-framework#1740 - CertificateInfo array element missing in identity application mgt wsdl

---

WSO2 Carbon 4.4.X Update 2018-07-24

This update provides capability to have multiple certificates for an identity provider for saml

Bug Fixes

- wso2/product-is#3295 - Allow two certificate for a identity provider

---

WSO2 Carbon 4.4.X Update 2018-07-24

This update provides capability to have multiple certificates for an identity provider for saml

Bug Fixes

- wso2/product-is#3295 - Allow two certificate for a identity provider

---

WSO2 Carbon 4.4.X Update 2018-08-01

Improvements in DCR endpoint and role based scope validation in token generation

Bug Fixes

- wso2/product-is#3354 - Validate scopes against user roles during token generation
- wso2/product-is#3446 - Provide REST API to retrieve oauth client data with SP name

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-08-01

This update is to introduce a property to append/not append user store
domain name with roles.

Bug Fixes

- wso2/product-is#3462 - Introduce a property to append/not append user store domain name with roles

---

WSO2 Carbon 4.4.X Update 2018-08-01

This update is used to move the OIDC discovery endpoint under the root
issuer/.well-known/openid-configuration

Bug Fixes

- wso2/product-is#3480 - Move the OIDC discovery endpoint under the root issuer/.well-known/openid-configuration

---

WSO2 Carbon 4.4.X Update 2018-08-01

According to the spec when trying to retrieve client details with non-existing client id server should respond with 401. At the moment it returns 403

Bug Fixes

- wso2/product-is#3493 - Fix DCR error code

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-08-01

This update removes /permission/admin/manage/identity/applicationmgt permission check while updating application owner.

Bug Fixes

- wso2/product-apim#3576 - Unable to generate Tokens For any user within a Tenant

---

WSO2 Carbon 4.4.X Update 2018-08-01

Remove all of distributed caching from the product core and provide capability to turn off it via configuration.
Use hazel cast messaging to invalidate local caches in a clustered environment.

Bug Fixes

- wso2/carbon-kernel#1774 - Remove distributed caching

Instructions

```
1.Instructions for local cache invalidation fix:
Stop the server.
Open <IS_HOME>/repository/conf/carbon.xml file and update the <Cache> element as follows,
<Cache>
<!-- Default cache timeout in minutes -->
<ForceLocalCache>true</ForceLocalCache>
<DefaultCacheTimeout>15</DefaultCacheTimeout>
</Cache>
Re-start the server
```

WSO2 Carbon 4.4.X Update 2018-08-08

When proxy is set, it cannot login into the admin application. This is because non proxy hosts are not considered when login happens. Auth manager call tries to go through the proxy and it fails.

Bug Fixes

- wso2/product-apim#3577 - Cannot login into the admin app when proxy is enabled

WSO2 Carbon 4.4.X Update 2018-08-08

This update fixes potential Cross-Site Scripting (XSS) vulnerabilities in org.wso2.carbon.identity.mgt.ui.jar

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0461

WSO2 Carbon 4.4.X Update 2018-08-08

This update fixes the NPE thrown when starting the server for the second time (Environment - Oracle database)

Bug Fixes

- wso2/product-is#3535 - NPE when starting the server for the second time. (Oracle database)

WSO2 Carbon 4.4.X Update 2018-08-08

Remove apache commons fileupload vulnerable jar from shindig and Upgrade fileupload version to 1.3.3

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0385

WSO2 Carbon 4.4.X Update 2018-08-11

This update fix the issues where the logout request destination does not match with the identityProviderLogoutURL, there is no validation for revokeTokensOfUserByAppResponse operation of APIKeyMgtSubscriberService and APIs does not get visible from store in distributed mode without clustering

Bug Fixes

- wso2/product-apim#3484 - APIs not getting visible from store in distributed mode without clustering
- wso2/carbon-apimgt#5571 - Logout request destination not matching with identityProviderLogoutURL
- wso2/carbon-apimgt#5573 - No validation for revokeTokensOfUserByAppResponse operation of APIKeyMgtSubscriberService

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-08-13

Exception occurs when invoking userinfo endpoint with a JWT token after oauth cache timeout

Bug Fixes

- wso2/product-is#3550 - Exception occurs when invoking userinfo endpoint with a JWT token after oauth cache timeout

Instructions

```
When applying the oauth2.war make sure to backup and remove the old extracted oauth2 folder.
```

WSO2 Carbon 4.4.X Update 2018-08-15

This update removes AuthenticationFilter from the entitlement endpoint as the authentication is already handled.

Bug Fixes

- wso2/product-is#3547 - Authentication fail for mutual SSL from Entitlement REST service layer

WSO2 Carbon 4.4.X Update 2018-08-15

This fix is to wait for externalCryptoProvider before calling the cryptoUtil by datasource component.

Bug Fixes

- wso2/product-ei#2533 - When there are datasources stored in the registry, a null pointer exception occurs at the server restart as a result of 'ServerConfigurationService' not created at the time of checking whether CryptoServiceEnabled from the update registry datasource operation.

WSO2 Carbon 4.4.X Update 2018-08-20

Upgrade apache cxf dependency version which has transitive dependency for cxf-rt-transports-http

Bug Fixes

- wso2/product-is#3597 - Upgrade CXF version

Instructions

```
When applying the war files make sure to backup and remove the old extracted war folders.
```

WSO2 Carbon 4.4.X Update 2018-08-24

This WUM update upgrades jackson dependencies to fix security vulnerabilities

Bug Fixes

- wso2/product-is#3603 - Upgrade jackson dependencies to fix security vulnerabilities

WSO2 Carbon 4.4.X Update 2018-08-24

Change jstl library and Remove xalan:serializer dependency

Bug Fixes

- wso2/product-is#3602 - Change jstl library to fix security vulnerabilities
- wso2/product-is#3622 - Remove xalan:serializer dependency since JDK ships it

Instructions

```
When applying the following war files make sure to backup and remove the corresponding old
extracted war folders.
shindig.war
emailotpauthenticationendpoint.war
smsotpauthenticationendpoint.war
x509certificateauthenticationendpoint.war
```

WSO2 Carbon 4.4.X Update 2018-08-24

This WUM update upgrades jackson-dataformat-xml dependencies to fix security vulnerabilities

Bug Fixes

- wso2/product-is#3603 - Upgrade jackson dependencies to fix security vulnerabilities

WSO2 Carbon 4.4.X Update 2018-08-27

BouncyCastle dependency is embedded in enant kerstore mgt and used for tenant certificate generation. We are using an old BC version which needs to be updated.

Bug Fixes

- wso2/product-is#3633 - Update bouncy castle version used in multitenancy

Instructions

```
-
```

WSO2 Carbon 4.4.X Update 2018-08-27

This update allows to set custom parameters in the access token response

Bug Fixes

- wso2/product-is#3194 - Allowing to set custom parameters in the access token response

Instructions

```
This update is copying a updated oauth2.war file into the <CARBON_HOME>/repository/deployment/server
/webapps/ folder. In order to let the new oauth2.war get extracted and affect to the server, backup
and delete the existing <CARBON_HOME>/repository/deployment/server/webapps/oauth2 folder, before
starting the server.
```

WSO2 Carbon 4.4.X Update 2018-08-29

Fixing the issue https://github.com/wso2/product-is/issues/3649

Bug Fixes

- wso2/product-is#3649 - Fix issue in scope binding to role fails with SQL exception in IS 5.5.0

Instructions

```
Follow below instructions to successfully apply the update
====================================================================================================

This update is copying updated oauth2.war file into the <CARBON_HOME>/repository/deployment/server
/webapps/ folder.

In order to let these updated files get extracted and affect the server, backup and delete existing
<CARBON_HOME>/repository/deployment/server/webapps/oauth2 folder, before starting the server.

Additionally backup and remove any other folders created as extraction of .war files, to make sure
any other updates having .war files are affected properly.
(Note: Make sure NOT to delete folders existed without .war files. Ex: Don't delete 'STRATOS_ROOT'
folder.)
```

WSO2 Carbon 4.4.X Update 2018-09-04

NPE while updating the application using soap

Bug Fixes

- wso2/product-is#3659 - NPE while updating the application using soap

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-09-04

This update will properly format the audit logs to print human readable values.

Bug Fixes

- wso2/product-apim#3641 - Audit log being printed while creating a role has all the permissions assigned to it. But the permissions are printed as a comma separated array elements, hence, unreadable. This should be printed in a more readable way.

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-09-04

This update fixes Multi part form-data file uploading issue in API Manager
2.2.0

Bug Fixes

- wso2/product-apim#1947 - Multi part form-data file uploading is getting failed in API Manager 2.2.0

Instructions

```
If your backend expects the multipart payload decoded (in plain text), set the following axis2
property in the in sequence,
<property name="DECODE_MULTIPART_DATA" scope="axis2" type="BOOLEAN" value="true"/>
You can use a mediation extension to set this property. See the following link on how to create a
mediation extension in API Manager 2.2.0,
https://docs.wso2.com/display/AM220/Adding+Mediation+Extensions
```

WSO2 Carbon 4.4.X Update 2018-09-04

This update adds Not before claim (NBF) to the JWT returned in 'token_string'
in introspection response.

Bug Fixes

- wso2/product-is#3681 - Add NBF to JWT 'token_string' in introspection response.

WSO2 Carbon 4.4.X Update 2018-09-07

Health Check API for Carbon based products.

Bug Fixes

- wso2/product-is#3693 - Health Check API for Carbon based products

Instructions

```
Carbon Health API check enables to check the health of a carbon product through an API.

To enable the feature change the following config to true in <CARBON_HOME>/repository/conf/health-
check-config.xml

<Enable>true</Enable>

This is an open API which is not secured. Hence if you enable this service please block this
service to outside.

Each health checker has it's own configurations. You can control the behavior through
configurations using above stated health-check-config file. (Enable, Disable and change the
execution order of health checkers, Change input parameters for each health checker)

Ex -
<HealthChecker name="DataSourceHealthChecker" orderId="97" enable="true">
<Property name="monitored.datasources">jdbc/WSO2CarbonDB,jdbc/WSO2MetricsDB,jdbc/WSO2UMDB</Property>
<Property name="pool.usage.limit.percentage">80</Property>
</HealthChecker>


To invoke api do a GET to the health-check API

curl -k -v https://{hostname}:{port}/api/health-check/v1.0/health
```

WSO2 Carbon 4.4.X Update 2018-09-08

This update will fix the issue mentioned in the git issue.

Bug Fixes

- wso2/product-apim#3656 - Role section is missing in the audit log when assigning default roles to users (e.g: Internal/publisher)

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-09-11

This update introduces the capability to log information related to OAuth
token generation in to a log file.

Bug Fixes

- wso2/product-is#3697 - Log token generation information

Instructions

```
To enable token information logging see the below instructions. Enabling this will create a log
file named 'transaction.log' at <IS_HOME>/repository/logs location.

1. Shutdown the server

2. Add the following to <IS_HOME>/repository/conf/log4j.properties file. This will set the log
configurations for transaction.log

log4j.logger.TRANSACTION_LOGGER=INFO, TRANSACTION_LOGGER
log4j.appender.TRANSACTION_LOGGER=org.apache.log4j.FileAppender
log4j.appender.TRANSACTION_LOGGER.File=${carbon.home}/repository/logs/transaction.log
log4j.appender.TRANSACTION_LOGGER.Append=true
log4j.appender.TRANSACTION_LOGGER.layout=org.apache.log4j.PatternLayout
log4j.appender.TRANSACTION_LOGGER.layout.ConversionPattern=[%d] - %m %n
log4j.appender.TRANSACTION_LOGGER.threshold=INFO
log4j.additivity.TRANSACTION_LOGGER=false

3. Add the following to <IS_HOME>/repository/conf/identity/identity.xml file under <EventListeners>
configuration. Logging can be disabled by setting enable="false".

<EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"
name="org.wso2.carbon.identity.data.publisher.oauth.listener.OAuthTokenIssuanceLogPublisher"
orderId="12" enable="true"/>

4. This update includes modifications to the oauth2 webapp which are included in oauth2.war. These
modifications are done only to java files and no jsp files are changed in this update.

If there is an 'oauth2' directory in the <IS_HOME>/repository/deployment/server/webapps directory
remove it. However, if there are customizations done to the oauth2 webapp make sure to add them
once the the new oauth2.war is exploded.

5. Once these changes are made, restart the server. If the changes are applied correctly, a log
file named ’transaction.log' will be created at <IS_HOME>/repository/logs location. Once you make
token generation related operations, they should be logged in the mentioned file.


A sample log entry will look like below.

[2018-09-07 18:56:48,335] - Type: OAUTH TOKEN | Info: {"expires_in_seconds":3327,"grant_type":"
password","success":true,"scope":"openid sc1","time_taken_in_millis":88,"issued_time":
1536326535993,"user":"admin@carbon.super","client_id":"_FNqderi6VQZ5eFHBkWsZQjl9yca"}


Following are some sample token generation related information which will be logged in different
scenarios

i. Successful token request

{
"expires_in_seconds":3327,
"grant_type":"password",
"success":true,
"scope":"openid scope1”,
"time_taken_in_millis":88,
"issued_time":1536326535993,
"user":"admin@carbon.super",
"client_id":"_FNqderi6VQZ5eFHBkWsZQjl9yca"
}

ii. Unsuccesful request to token endpoint

{
"grant_type":"password",
"error_description":"Authentication failed for admin",
"success":false,
"scope":"scope1 openid",
"error":"invalid_grant",
"user":"admin@carbon.super",
"client_id":"_FNqderi6VQZ5eFHBkWsZQjl9yca"
}

iii. Unsuccessful request to authorize endpoint

{
"error_description":"A valid OAuth client could not be found for client_id:
```

```
_FNqderi6VQZ5eFHBkWsZQjl9yca1",
"success":false,
"scope":"openid",
"response_type":"token",
"error":"invalid_client",
"client_id":"_FNqderi6VQZ5eFHBkWsZQjl9yca1"
}
```

WSO2 Carbon 4.4.X Update 2018-09-19

This Fix multiple issues mentioned in bug fixes.

Bug Fixes

- wso2/product-apim#3714 - Cannot Edit a Service Provider on Carbon Console
- wso2/wso2-axiom#39 - Replace illegal characters sent in XML payload

WSO2 Carbon 4.4.X Update 2018-09-25

This update will fix the issue where double submits in login page may skip the second factor of the authentication.

Instructions

```
Follow below instructions to successfully apply the update
====================================================================================================

This update is copying updated authenticationendpoint.war file into the <CARBON_HOME>/repository
/deployment/server/webapps/ folder.

In order to let these updated files get extracted and affect the server, backup and delete existing
<CARBON_HOME>/repository/deployment/server/webapps/authenticationendpoint folder, before starting
the server.

Additionally backup and remove any other folders created as extraction of .war files, to make sure
any other updates having .war files are affected properly.
(Note: Make sure NOT to delete folders existed without .war files. Ex: Don't delete 'STRATOS_ROOT'
folder.)
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0473

WSO2 Carbon 4.4.X Update 2018-09-25

This WUM update facilitates adding ReCaptcha for account recovery, that is, forgot username and password scenarios.

Bug Fixes

- wso2/product-is#3777 - Need to Support Captcha Validation for Account Recovery

Instructions

```
1. Set up reCaptcha with the WSO2 Identity Server. For instructions on how to do this and more
information about reCaptcha, see Setting Up ReCaptcha.
2. Start the WSO2 Identity Server and log in to the management console.
3. Click on List under Identity Providers on the Main tab and then click Resident Identity
Provider.
```

```
4. Expand the Account Management Policies tab and then expand the Account Recovery tab.
5. Select the Enable reCaptcha checkbox to enable reCaptcha for the username recovery/password
recovery flow.
```

WSO2 Carbon 4.4.X Update 2018-09-28

This update will fix aforementioned git issues.

Bug Fixes

- wso2/product-is#3778 - Unable to add Application role to a user when the Primary Userstore is ReadOnlyAD
- wso2/product-is#3779 - IndexOutOfBoundsException occur when displayNames parameter becomes Empty

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-09-28

This update fixes an issue with refreshed access tokens that generated with SAML 2 bearer grant in LEGACY mode, which causes the issue 'Invalid Domain Name' when generating JWT that is send to backend by api manager gateway.

Bug Fixes

- wso2/product-apim#3750 - Invalid Domain Name error when generating the JWT

WSO2 Carbon 4.4.X Update 2018-10-08

This update changing the structure of the identity XML file to enable reCaptcha for account recovery.

Bug Fixes

- wso2/product-is#3777 - Need to Support Captcha Validation for Account Recovery.

Instructions

```
1. You can enable the reCaptcha using management console, where management console -> Identity
Providers -> Resident Identity Provider ->
Account Management Policies tab -> Account Recovery tab, then,
select the Enable reCaptcha checkbox to enable reCaptcha for the username recovery/password
recovery flow.
2. Otherwise, if you wish to configure account recovery reCaptcha globally then,
Navigate to the <IS_HOME>/repository/conf/identity/identity.xml file and add the following
ReCaptcha configurations under the recovery block.
Tip: To avoid any configuration issues, do this before starting up the WSO2 Identity Server product
instance.
<Recovery>
<ReCaptcha>
<Password>
<Enable>true</Enable>
</Password>
<Username>
<Enable>true</Enable>
</Username>
</ReCaptcha>
```

```
.............
</Recovery>
```

WSO2 Carbon 4.4.X Update 2018-10-08

The WSO2 in-place updates tool allows you to update your currently used product by fetching updates from the server and merging all configurations and files. The tool also gives backup and restore capability.

Bug Fixes

- wso2/carbon-kernel#1861 - Add In-place updates client

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-10-08

This update contains the fixes for returning 406 when Accept apication/scim json header included , ResourceTypes endpoint implemented as ResourceType ,Malformed ListResponse from resourcetype endpoint and it allows to include primary phone boolean

Bug Fixes

- wso2/product-is#3371 - ResourceTypes endpoint implemented as ResourceType
- wso2/product-is#3372 - Malformed ListResponse from resourcetype endpoint
- wso2/product-is#3374 - 406 Not Acceptable returned when Accept application/scim json header include
- wso2/product-is#3571 - Including primary phone boolean flag in user creation causes org.apache.cxf.interceptor. Fault and returns it to requestor

WSO2 Carbon 4.4.X Update 2018-10-08

This update contains the Mutual TLS with Id secret connector in the default WUM pack.

Bug Fixes

- wso2/product-is#3805 - Adding Mutual TLS with Id secret connector in the default pack

WSO2 Carbon 4.4.X Update 2018-10-11

Set the user store domain properly.

Bug Fixes

- wso2/product-is#3813 - User store domain is not properly set in the challenge question path

Instructions

```
Replace api#identity#recovery#v0.9.war
```

WSO2 Carbon 4.4.X Update 2018-10-13

This update fixes the issue with illegal character in XML payloads by
replacing illegal characters.

Bug Fixes

- wso2/wso2-axiom#39 - Replace illegal characters sent in XML payload

Instructions

```
If the file 'XMLOutputFactory.properties' does not exist in the
<PRODUCT_HOME> directory create the file. Add the following entry to the
'XMLOutputFactory.properties' to replace illelgal XML characters with spaces.
com.ctc.wstx.outputInvalidCharHandler.char=u0020
```

WSO2 Carbon 4.4.X Update 2018-10-16

'This update fixes the issues with 406 Not Acceptable returned when Accept: application/scim+json header included and IS SCIM2 addresses mapping issues'

Bug Fixes

- wso2/product-is#3374 - 406 Not Acceptable returned when Accept: application/scim+json header included
- wso2/product-is#3802 - IS SCIM2 addresses mapping
- wso2/product-is#3823 - Primary flag for email and phone number as per SCIM 2.0 spec

Instructions

```
This is applied for the issue [1]
It is required to start the server with the following system property to apply the fix of issue [1].
-Dscim2.compliance=true
[1] https://github.com/wso2/product-is/issues/3374

This is applied for the issue [2] and [3]
With this update, SCIM 2.0 complex multivalued attributes will be converted to distinct claims and
will be able to store and retrieve properly.
For an example, an attribute like 'addresses', it could have canonical type values of 'work' and
'home'. And the value attribute is a complex type consists with sub-attributes 'formatted',
'streetAddress', 'postalCode' etc.
In order to store different sub attributes of the different canonical types values, its needed to
create distinct claims in the SCIM dialect. To do so, add external claims in 'urn:ietf:params:scim:
schemas:core:2.0:User' dialect in
following format,
urn:ietf:params:scim:schemas:core:2.0:User:addresses#work.formatted
urn:ietf:params:scim:schemas:core:2.0:User:addresses#work.streetAddress
urn:ietf:params:scim:schemas:core:2.0:User:addresses#work.primary
urn:ietf:params:scim:schemas:core:2.0:User:addresses#work.postalCode
urn:ietf:params:scim:schemas:core:2.0:User:addresses#home.formatted
urn:ietf:params:scim:schemas:core:2.0:User:addresses#home.streetAddress
urn:ietf:params:scim:schemas:core:2.0:User:addresses#home.postalCode
urn:ietf:params:scim:schemas:core:2.0:User:addresses#home.primary
with matching 'Mapped Local Claim' URI in the local dialect. If you have more sub-attributes or
type values, you have to follow the same pattern and add more external claims.
Additionally, to enable this functionality, you have to add below configuration in identity.xml.
<Server>
```

```
...
<SCIM2>
...
<ComplexMultiValuedAttributeSupportEnabled>true</ComplexMultiValuedAttributeSupportEnabled>
</SCIM2>
...
</Server>
Please note that, without enabling this flag, Identity Server store and retrieve only one value for
a given multivalued complex attribute.

For an example, an attribute like 'addresses', Identity Server will store sub attribute values
under following claims,
urn:ietf:params:scim:schemas:core:2.0:User:addresses.formatted
urn:ietf:params:scim:schemas:core:2.0:User:addresses.streetAddress
urn:ietf:params:scim:schemas:core:2.0:User:addresses.postalCode
where it does not have the canonical type qualifier to distinguish the canonical type. Where as,
with enabling this flag, it will store and retrieve values from the claims with the format
specified initially.
So, if you are currently using multivalued complex attributes types such as 'addresses','emails'
attributes without any issue, it is advised to not to enable this flag as this change the data
storing pattern for users which need
separate data migration for an existing deployment.
[2]https://github.com/wso2/product-is/issues/3802
[3]https://github.com/wso2/product-is/issues/3823
```

WSO2 Carbon 4.4.X Update 2018-10-18

This update generates logs for OAuth introspection endpoint similar to the OAuth token endpoint.

Bug Fixes

- wso2/product-is#3822 - Log Generation for OAuth2 Introspection Endpoint

Instructions

```

Follow the below instructions to enable the log for Introspection endpoint.

Enabling this will create a log file named 'transaction.log' at <IS_HOME>/repository/logs location.
1. Shutdown the server
2. Add the following to <IS_HOME>/repository/conf/log4j.properties file. This will set the log
configurations for transaction.log

log4j.logger.TRANSACTION_LOGGER=INFO, TRANSACTION_LOGGER
log4j.appender.TRANSACTION_LOGGER=org.apache.log4j.FileAppender
log4j.appender.TRANSACTION_LOGGER.File=${carbon.home}/repository/logs/transaction.log
log4j.appender.TRANSACTION_LOGGER.Append=true
log4j.appender.TRANSACTION_LOGGER.layout=org.apache.log4j.PatternLayout
log4j.appender.TRANSACTION_LOGGER.layout.ConversionPattern=[%d] - %m %n
log4j.appender.TRANSACTION_LOGGER.threshold=INFO
log4j.additivity.TRANSACTION_LOGGER=false

3. Add the following to <IS_HOME>/repository/conf/identity/identity.xml file under <EventListeners>
configuration.
Logging can be disabled by setting enable="false".
Optinally, you enable the "Log.Token" property if want to log the token as well.
<EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"
name="org.wso2.carbon.identity.data.publisher.oauth.listener.OAuthTokenIssuanceLogPublisher"
orderId="12" enable="true">
<Property name="Log.Token">false</Property>
</EventListener>
```

WSO2 Carbon 4.4.X Update 2018-10-18

This update supports for refersh token instrospection and token_type_hint

Bug Fixes

- wso2/product-is#3780 - Supporting refresh tokens for introspection supporting token_type_hint parameter

WSO2 Carbon 4.4.X Update 2018-10-25

Implement scim filtering enhancements

Bug Fixes

- wso2/product-is#3831 - Add a property to return always "DOMAIN/userName" regardless of primary or secondary userstore in response when SCIM api get called.

Instructions

```
If filtering enhancements are enabled,
To get users from a user store other than the primary user store you have to provide domain name in
the username.

Contains filter is added for SCIM filtering.
https://localhost:9443/scim2/Users?filter=userName+co+<username>

Filtering enhancements can be enabled by adding the following property to identity.xml under scim2
<EnableFilteringEnhancements>true</EnableFilteringEnhancements>
```

WSO2 Carbon 4.4.X Update 2018-10-25

This update provides support for encrypted SAML assertion in SSO

Bug Fixes

- wso2/analytics-apim#590 - Unable to login to the management console with encrypted SAML Assertion

WSO2 Carbon 4.4.X Update 2018-10-25

This update contains fixes for stored XSS vulnerability in Add User Store page description field.

Please note that this is a security update. For more information please view Security Advisory WSO2-2017-0197

WSO2 Carbon 4.4.X Update 2018-11-05

This update adds correlation logs for JDBC and LDAP calls

Bug Fixes

- wso2/carbon-kernel#1863 - Adding correlation logs for JDBC and LDAP calls

Instructions

```
Add below code set to the <CARBON_SERVER>/repository/conf/log4j.properties file and save.
# Appender config to put correlation Log.
log4j.logger.correlation=INFO, CORRELATION
log4j.additivity.correlation=false
```

```
log4j.appender.CORRELATION=org.apache.log4j.RollingFileAppender
log4j.appender.CORRELATION.File=${carbon.home}/repository/logs/${instance.log}/correlation.log
log4j.appender.CORRELATION.MaxFileSize=10MB
log4j.appender.CORRELATION.layout=org.apache.log4j.PatternLayout
log4j.appender.CORRELATION.Threshold=INFO
log4j.appender.CORRELATION.layout.ConversionPattern=%d{yyyy-MM-dd HH:mm:ss,SSS}|%X{Correlation-ID}|%
t|%m%n
Add below system property to the <CARBON_SERVER>/bin/wso2server.sh and save. By default this logs
are disabled. Set this value to true for enable the feature.
-DenableCorrelationLogs=false \
Add below value under <Host> tag in <CARBON_SERVER>/repository/conf/tomcat/catalina-server.xml and
save.
<Valve className="org.wso2.carbon.tomcat.ext.valves.RequestCorrelationIdValve"
headerToCorrelationIdMapping="{'activityid':'Correlation-ID'}" queryToCorrelationIdMapping="
{'RelayState':'Correlation-ID'}"/>
Sample files with above mention changes contains in resource folder.
(This is only sample files. Do not copy this files to the product folder)
```

WSO2 Carbon 4.4.X Update 2018-11-07

Service providers with same authentication mechanism are not SSO-ed when authenticator name is different. This mainly affect the basic authenticator and the request path authenticator.

Bug Fixes

- wso2/product-is#3882 - Service providers with same authentication mechanism are not SSO-ed when authenticator name is different

Instructions

```
Add "AuthMechanism" parameter to "BasicAuthenticator" and "BasicAuthRequestPathAuthenticator"
config entries in <CARBON_HOME>/repository/conf/identity/application-authentication.xml file. Use
"basic" as the value.

Sample config elements would look like below.

<AuthenticatorConfig name="BasicAuthenticator" enabled="true">
<Parameter name="AuthMechanism">basic</Parameter>
</AuthenticatorConfig>
<AuthenticatorConfig name="BasicAuthRequestPathAuthenticator" enabled="true" >
<Parameter name="AuthMechanism">basic</Parameter>
</AuthenticatorConfig>
```

WSO2 Carbon 4.4.X Update 2018-11-07

This update provides the abilitiy to perform an intermidate certificate validation for certificate based requests.

Instructions

```
Add the following config to the <IS_home>/repository/conf/identity/identity.xml file inside the
<Server xmlns="http://wso2.org/projects/carbon/carbon.xml"> tag.
To enable the intermediate certificate validation change enable="false" to enable="true" as follows
<IntermediateCertValidation enable="true">.
Add the intermediate certificate CN in the <CertCN> element. Multiple <CertCN> elements can be used
for multiple certificates.
Add exemptable context paths from this validation in the <Context> elemet. Multiple <Context>
elements can be used for multiple contexts.

<IntermediateCertValidation enable="false">
<IntermediateCerts>
<!--Add intermediate certificate CN. Multiple <CertCN> elements can be used for multiple
certificates.-->
<CertCN>localhost</CertCN>
</IntermediateCerts>
```

```
<ExemptContext>
<!--Add exemptable context paths. Multiple <Context> elements can be used for multiple contexts.-->
<!-- <Context>oauth2</Context> -->
</ExemptContext>
</IntermediateCertValidation>

The incoming certificate request CN should be the username of the user and the certificate issuer
CN should be in a <CertCN> tag.
If a context path is required to be exempted from the validation that context can be added with a
<Context> tag.
Restart the server after applying the config.
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0492

WSO2 Carbon 4.4.X Update 2018-11-10

This update introduces a property to mandate Mutual SSL in tlswithidsecret authenticator

Bug Fixes

- wso2/product-is#3944 - Add a property to mandate Mutual SSL in tlswithidsecret authenticator

WSO2 Carbon 4.4.X Update 2018-11-15

Fix issue in adding Challenge Questions

Bug Fixes

- wso2/product-is#3939 - Challenge Questions Set cannot add after delete all existing challenge questions

WSO2 Carbon 4.4.X Update 2018-11-24

This update fixes authorization issues with ChallengeQuestionManagementAdminService setUserChallengeAnswers operation

Bug Fixes

- wso2/product-is#3871 - Authorization issues with ChallengeQuestionManagementAdminService setUserChallengeAnswers operation

WSO2 Carbon 4.4.X Update 2018-11-26

Implement SAML metdata enhancements by providing,
1) Configure validity time through UI
2) Add destination URL's to metadata response
3) Add "WantAuthnRequestsSigned" in IDPSSODescriptor
4) sign the Resident IdP SAML metadata

Bug Fixes

- wso2/product-is#3884 - UI feature to set the validity period of 'validUntil' tag of Resident IDP SAML metadata returned

Instructions

```
Add the following configuration to your your identity.xml in IS_HOME/repository/conf/identity
/identity.xml

<SAMLMetadataValidityPeriod>60</SAMLMetadataValidityPeriod>
<SAMLMetadataSigningEnabled>false</SAMLMetadataSigningEnabled>
```

WSO2 Carbon 4.4.X Update 2018-11-26

Implement SAML metdata enhancements by providing,
1) Configure validity time through UI
2) Add destination URL's to metadata response
3) Add "WantAuthnRequestsSigned" in IDPSSODescriptor
4) sign the Resident IdP SAML metadata

Bug Fixes

- wso2/product-is#3884 - UI feature to set the validity period of 'validUntil' tag of Resident IDP SAML metadata returned

Instructions

```
Add the following configuration to your your identity.xml in IS_HOME/repository/conf/identity
/identity.xml

<SAMLMetadataValidityPeriod>60</SAMLMetadataValidityPeriod>
<SAMLMetadataSigningEnabled>false</SAMLMetadataSigningEnabled>
```

WSO2 Carbon 4.4.X Update 2018-11-26

Implement SAML metdata enhancements by providing,
1) Configure validity time through UI
2) Add destination URL's to metadata response
3) Add "WantAuthnRequestsSigned" in IDPSSODescriptor
4) sign the Resident IdP SAML metadata

Bug Fixes

- wso2/product-is#3884 - UI feature to set the validity period of 'validUntil' tag of Resident IDP SAML metadata returned

Instructions

```
Add the following configuration to your your identity.xml in IS_HOME/repository/conf/identity
/identity.xml

<SAMLMetadataValidityPeriod>60</SAMLMetadataValidityPeriod>
<SAMLMetadataSigningEnabled>false</SAMLMetadataSigningEnabled>
```

WSO2 Carbon 4.4.X Update 2018-11-27

Implement SAML metdata enhancements by providing,
1) Configure validity time through UI
2) Add destination URL's to metadata response
3) Add "WantAuthnRequestsSigned" in IDPSSODescriptor
4) sign the Resident IdP SAML metadata

Bug Fixes

- wso2/product-is#3884 - UI feature to set the validity period of 'validUntil' tag of Resident IDP SAML metadata returned

Instructions

```
Add the following configuration to your your identity.xml in IS_HOME/repository/conf/identity
/identity.xml

<SAMLMetadataValidityPeriod>60</SAMLMetadataValidityPeriod>
<SAMLMetadataSigningEnabled>false</SAMLMetadataSigningEnabled>
```

WSO2 Carbon 4.4.X Update 2018-11-27

Implement SAML metdata enhancements by providing,
1) Configure validity time through UI
2) Add destination URL's to metadata response
3) Add "WantAuthnRequestsSigned" in IDPSSODescriptor
4) sign the Resident IdP SAML metadata

Bug Fixes

- wso2/product-is#3884 - UI feature to set the validity period of 'validUntil' tag of Resident IDP SAML metadata returned

Instructions

```
Add the following configuration to your your identity.xml in IS_HOME/repository/conf/identity
/identity.xml

<SAMLMetadataValidityPeriod>60</SAMLMetadataValidityPeriod>
<SAMLMetadataSigningEnabled>false</SAMLMetadataSigningEnabled>
```

WSO2 Carbon 4.4.X Update 2018-11-27

This update provides the fix to add support for configuring SSL protocols and ciphers in ThriftAuthenticationService (port 10711).

Instructions

```
N/A
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0459

WSO2 Carbon 4.4.X Update 2018-11-28

Adding html encoding for displayPath attribute value in resource_tree_ajaxprocessor.jsp

Instructions

```
N/A
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0405

WSO2 Carbon 4.4.X Update 2018-11-28

This update adds correlation logs for JDBC and LDAP calls

Bug Fixes

- wso2/carbon-kernel#1863 - Adding correlation logs for JDBC and LDAP calls

Instructions

```
Add below code set to the <CARBON_SERVER>/repository/conf/log4j.properties file and save.
# Appender config to put correlation Log.
log4j.logger.correlation=INFO, CORRELATION
log4j.additivity.correlation=false
log4j.appender.CORRELATION=org.apache.log4j.RollingFileAppender
log4j.appender.CORRELATION.File=${carbon.home}/repository/logs/${instance.log}/correlation.log
log4j.appender.CORRELATION.MaxFileSize=10MB
log4j.appender.CORRELATION.layout=org.apache.log4j.PatternLayout
log4j.appender.CORRELATION.Threshold=INFO
log4j.appender.CORRELATION.layout.ConversionPattern=%d{yyyy-MM-dd HH:mm:ss,SSS}|%X{Correlation-ID}|%
t|%m%n
Add below system property to the <CARBON_SERVER>/bin/wso2server.sh and save. By default this logs
are disabled. Set this value to true for enable the feature.
-DenableCorrelationLogs=false \
Add below value under <Host> tag in <CARBON_SERVER>/repository/conf/tomcat/catalina-server.xml and
save.
<Valve className="org.wso2.carbon.tomcat.ext.valves.RequestCorrelationIdValve"
headerToCorrelationIdMapping="{'activityid':'Correlation-ID'}" queryToCorrelationIdMapping="
{'RelayState':'Correlation-ID'}"/>
Sample files with above mention changes contains in resource folder.
(This is only sample files. Do not copy this files to the product folder)
```

WSO2 Carbon 4.4.X Update 2018-11-28

This update improves error messages in IdentityApplicationManagement SOAP API.

Bug Fixes

- wso2/product-is#4040 - WSO2 IS - IdentityApplicationManagement SOAP API giving generic error

WSO2 Carbon 4.4.X Update 2018-12-05

The parameter '''mediaType''' in components/registry/org.wso2.carbon.registry.resource.ui/src/main/resources/web/resources/metadata_resourcepath.jsp, components/registry/org.wso2.carbon.registry.resource.ui/src/main/resources/web/resources

/metadata_ajaxprocessor.jsp and components/registry/org.wso2.carbon.registry.resource.ui/src/main/resources/web/resources/raw-collection-content.jsp have not encoded.

Instructions

```
N/A
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0422

WSO2 Carbon 4.4.X Update 2018-12-05

This update fixes password reset via email not working for tenant users and checking the availability of SP_CLAIM_DIALECT does not work properly with mysql

Bug Fixes

- wso2/product-is#4076 - Password reset via email not working for tenant users

WSO2 Carbon 4.4.X Update 2018-12-07

Use InternalKeystore for encryption if it's configured

Bug Fixes

- wso2/product-is#4071 - Enable changing encryption keystore in Cipher-tool

WSO2 Carbon 4.4.X Update 2018-12-07

Make signing and digest algorithms used by SAML token issuer configurable

Instructions

```
Add the following configuration under security in carbon.xml

<STSSignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</STSSignatureAlgorithm>
<STSDigestAlgorithm>http://www.w3.org/2001/04/xmlenc#sha256</STSDigestAlgorithm>

Restart the server.
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0517

WSO2 Carbon 4.4.X Update 2018-12-09

NPE in getting resident IDP in certain scenarios

Bug Fixes

- wso2/product-is#4148 - NPE in getting resident IDP in certain scenarios

WSO2 Carbon 4.4.X Update 2018-12-14

This update resolves the error when including '\b' and '\f' reserved characters within XML in ESB-5.0.0.

Bug Fixes

- wso2/product-ei#2932 - JSON Reserved Characters \b and \f are not Handle Properly Within the XML

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2018-12-20

This update fixes the OAuth2 token validation logic to be compatible with custom token issuer extensions

Bug Fixes

- wso2/product-is#4190 - Custom JWT token issuer is not considered during token validation

WSO2 Carbon 4.4.X Update 2019-01-08

With this improvement we provide the capability to,
Turn off any authentication handler at System level. (In identity.xml)
Change the priority of any authentication handler at System level. (In identity.xml)
Enforce authentication mechanisms per resource.

Bug Fixes

- wso2/product-is#3169 - Improve Authentication Rest Valve to enforce client authentication mechanism per resource

Instructions

```
Turn off any authentication handler at System level. (In identity.xml)
...
<EventListeners>
<EventListener enable="false"
name="org.wso2.carbon.identity.auth.service.handler.impl.
ClientCertificateBasedAuthenticationHandler"
orderId="1000" type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler"/>
...
</EventListeners>
...

Change the priority of any authentication handler at System level. (In identity.xml)
...
<EventListeners>
<EventListener enable="true"
name="org.wso2.carbon.identity.auth.service.handler.impl.BasicAuthenticationHandler"
orderId="1" type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler"/>
```

```
...
</EventListeners>
...

Enforce authentication mechanisms per resource. (In identity.xml)
...
<ResourceAccessControl>
...
<Resource context="(.*)/usermanagement/v1/user/(.*)" http-method="all" secured="true" allowed-auth-
handlers="BasicAuthentication,OAuthAuthentication">
</Resource>
...
</ResourceAccessControl>
...

When 'allowed-auth-handlers' attribute is not defined all available authentication handlers will be
engaged to the resource
```

WSO2 Carbon 4.4.X Update 2019-01-08

This Fix not to create logger when update with non existing logger name

Bug Fixes

- wso2/product-apim#4120 - Create Loggers when updating a logger with invalid name using LoggingAdmin service

WSO2 Carbon 4.4.X Update 2019-01-08

Upgrade the commons-fileupload version

Instructions

```
N/A
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0385

WSO2 Carbon 4.4.X Update 2019-01-14

This update contains a fix related to tenant creation

Bug Fixes

- wso2/product-is#4266 - Fix tenant creation failure

WSO2 Carbon 4.4.X Update 2019-01-16

Fixing SCIM2 Unable to list multi-valued attributes via SCIM2 filter operation and fixed filter based on numeric values.

Bug Fixes

- wso2/product-is#3073 - Unable to list multi-valued attributes via SCIM2 filter operation

- wso2/product-is#3075 - Unable to filter based on numeric values in SCIM2

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2019-01-22

Fix issues in SCIM patch operation when ComplexMultiValuedAttributeSupportEnabled is enabled

Bug Fixes

- wso2/product-is#4310 - SCIM2 PATCH/PUT operations are failing

WSO2 Carbon 4.4.X Update 2019-01-29

Fixing store layout gets corrupted after page refresh and admin jaggeryapp does not respect http. nonProxyHosts

Bug Fixes

- wso2/product-apim#4194 - APIM Store layout gets corrupted after page refresh
- wso2/product-apim#4217 - APIM 2.6.0 admin jaggeryapp does not respect http.nonProxyHosts

WSO2 Carbon 4.4.X Update 2019-01-29

This update is to fix SAML binding information in the IdP SAML metadata to urn:oasis:names:tc: SAML:2.0:bindings:SOAP and append tenantDomain parameter to the endpoints for IdP tenants other than super tenant.

Bug Fixes

- wso2/product-is#4341 - saml metadata not correct for singleLogout service

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2019-01-29

This update is to fix SAML binding information in the IdP SAML metadata to urn:oasis:names:tc: SAML:2.0:bindings:SOAP and append tenantDomain parameter to the endpoints for IdP tenants other than super tenant.

Bug Fixes

- wso2/product-is#4341 - saml metadata not correct for singleLogout service

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2019-02-02

Bug in Siddhi which validates app successfully when the prefix is not defined

Bug Fixes

- wso2/product-sp#914 - Bug in Siddhi which validates app successfully when the prefix is not defined

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2019-02-06

This update upgrades BouncyCastle dependency to version 1.60, in order to mitigate the reported security vulnerabilities in lower versions

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0537

WSO2 Carbon 4.4.X Update 2019-02-06

This update fixes the issue where there are two user-store as PRIMARY and EXTERNAL and SCIM is only enabled for External user store, /scim2/Users rest call does not work

Bug Fixes

- wso2/product-is#4388 - Enabling SCIM only for specific user stores resulting in internal server error

---

WSO2 Carbon 4.4.X Update 2019-02-09

This update upgrades BouncyCastle dependency to version 1.60, in order to mitigate the reported security vulnerabilities in lower versions.

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0537

WSO2 Carbon 4.4.X Update 2019-02-09

This update fixes an error related to resolving the keystore file path, occurred when running ciphertool.bat with option -Dconfigure.

Bug Fixes

- wso2/cipher-tool#43 - Cipher Tool throws java.nio.file.InvalidPathException Illegal char <:> in Windows

Instructions

```
N/A
```

WSO2 Carbon 4.4.X Update 2019-02-15

This update fixes the issue 'isFederated' flag is not set for authorized user with JWT Bearer Grant when the token info is taken from the database.

Bug Fixes

- wso2/product-is#4417 - isFederated flag is not set for authorized user with JWT Bearer Grant when the token info is taken from the database.

WSO2 Carbon 4.4.X Update 2019-02-15

This update fixes the issue SCIM2 lists admin in full `/Users` list, but not when specifically requested

Bug Fixes

- wso2/product-is#4415 - SCIM2 lists admin in full `/Users` list, but not when specifically requested

---

WSO2 Carbon 4.4.X Update 2019-02-27

This fix will solves the issue when using multiple recipients in saml bearer grant type

Bug Fixes

- wso2/product-is#3754 - Recipient validation fails with multiple recipients in saml bearer grant type

Instructions

```
None
```

WSO2 Carbon 4.4.X Update 2019-02-27

This update fixes the issue enabling SCIM only for specific user stores resulting in internal server error with Groups endpoint.

Bug Fixes

- wso2/product-is#4388 - Fix enabling SCIM only for specific user stores resulting in internal server error with Groups endpoint

WSO2 Carbon 4.4.X Update 2019-02-27

Changing the claim dialect URI in Azure AD authenticator.

Bug Fixes

- wso2-extensions/identity-outbound-auth-office365#12 - fix the Azure AD authenticator to comply with OpenID protocol

WSO2 Carbon 4.4.X Update 2019-03-05

add more debug logs to entitlement module

Bug Fixes

- wso2/product-is#4486 - Need to provide more debug logs in carbon-identity-framework,entitlement module

WSO2 Carbon 4.4.X Update 2019-03-07

Even if user is removed the remember me session is still active. This fix Verify authenticated user retrieved from cache.

Please note that this is a security update. For more information please view Security Advisory WSO2-2018-0488

WSO2 Carbon 4.4.X Update 2019-03-12

This update is to validate the callback URL passed to the recovery endpoint during account recovery and self registration flows.

Instructions

```
This update introduces an option to configure callback URL regex for account recovery and self
registration to validate the callback URL in the request. Callback URL regex can be configured in
the management console or identity.xml file. Please find the below details on the callback URL
regex configuration.

1. Configure through management console,
- Login to the management console and navigate to 'Identity Providers -> Resident -> Account
Management Policies -> Account Recovery/User self registration'
- Enter the callback URL regex in the fields, 'Recovery callback URL regex' for account recovery
and 'User self registration callback URL regex' for self registration scenarios
- Click on 'Update'

2. Configure through file,
- Open the file identity.xml located at <IS_HOME>/repository/conf/identity
- Add the callback URL regex with the tag <CallbackRegex> user the tags <Recovery> for account
recovery and <SelfRegistration> for self registration scenarios
Eg-
<Recovery>
...
<CallbackRegex>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint
/login.do</CallbackRegex>
```

```
</Recovery>

<SelfRegistration>
...
<CallbackRegex>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint
/login.do</CallbackRegex>
</SelfRegistration-->
- Restart the server
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2019-0545

WSO2 Carbon 4.4.X Update 2019-03-12

This update is to upgrade Open SAML version to 2.6.6

Please note that this is a security update. For more information please view Security Advisory WSO2-2019-0572

WSO2 Carbon 4.4.X Update 2019-03-13

This update fixes the issue SP creation fails when the base64 encoded value of SAML issuer contains slash.

Bug Fixes

- wso2/product-is#4554 - SP creation fails when the base64 encoded value of SAML issuer contains slash

WSO2 Carbon 4.4.X Update 2019-03-17

When using the Security Token Service (STS) if the client sends a wrong username or password (authentication failure), rampart module will throw an AxisFault and it'll be logged as an exception. Since this is an application error, such error log is unneccessary. This update has modified the rampart module to thow an AxisFault with AxisFaultType set to Application Fault, so that the axis level will not log the exception.

Bug Fixes

- wso2/product-is#4571 - Print a stack trace for an unsuccessful login request.

WSO2 Carbon 4.4.X Update 2019-03-19

This update is to upgrade commons-codec dependency version to 1.12

Please note that this is a security update. For more information please view Security Advisory WSO2-2019-0577

WSO2 Carbon 4.4.X Update 2019-03-24

This update fixes 'Application/* roles are getting removed upon federated users re-login to servers'

Bug Fixes

- wso2/product-apim#4402 - Application/* roles are getting removed upon federated users re-login to servers

Instructions

```
Follow below steps to apply the fix
1. Open <WSO2_HOME>/repository/conf/identity/application-authentication.xml
2. Update '<ProvisioningHandler>' config to 'org.wso2.carbon.identity.application.authentication.
framework.handler.provisioning.impl.SystemRolesRetainedProvisionHandler'
3. Save the changes.
```

WSO2 Carbon 4.4.X Update 2019-03-26

This update removes the groovy jar from plugins

Instructions

```
Just getting the wum update will work. (We can make sure this by checking plugins folder for groovy
jar)
```

Please note that this is a security update. For more information please view Security Advisory WSO2-2019-0582

WSO2 Carbon 4.4.X Update 2019-03-28

This update fixes the aforementioned git issues.

Bug Fixes

- wso2/product-is#4818 - Refresh token generate username with blank space
- wso2/product-is#1352 - Make username trimming consistent across all UserStoreManager classes

Instructions

```
N/A
```

Security Advisories

Security Advisory WSO2-2017-0197

Overview

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

Description

This vulnerability is discovered in the Add User Store page in the Management Console. However, exploiting the vulnerability remotely is not possible as the malicious script should be injected to a textbox after accessing the web page in the user's browser where the script would run as a result of a javascript event bound to the text box.

Severity

Low

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 WSO2-2018-0385

Overview

Fixing the CVE-2016-3092 reported on Apache Commons FileUpload dependency library.

Description

With this fix, the commons-fileupload.1.3.1.jar packed to the product is removed. In addition to that, the orbit bundle commons-fileupload 1.3.2.wso2v1 which depends on 1.3.2 version is upgraded to be dependent on 1.3.3 version, which is not reported to be vulnerable.

Severity

High

Impact

The vulnerability may lead to a potential denial of service (DoS) attack via a long boundary string.

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 WSO2-2018-0405

Overview

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

Description

This vulnerability can be exploited in the registry UI of the Management Console by sending an HTTP GET request with a harmful request parameter.

Severity

Low

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 WSO2-2018-0422

Overview

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

Description

This addresses a potential XSS vulnerability identified in Management Console(In Registry)and it has been identified that two such prameters displayed in the HTML page result were not properly encoded before displyaing.

Severity

Low

Impact

By performing a Stored 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 WSO2-2018-0447

Overview

WSO2 products are found to be vulnerable to arbitrary file write via an archive.

Description

An attacker would be able to exploit the vulnerability [1] by specially crafting a malicious archive file that can be uploaded to the WSO2 server.

[1] https://snyk.io/research/zip-slip-vulnerability

Severity

Medium

Impact

By successfully exploiting the vulnerability, an attacker having required permissions would be able to add or overwrite files in to the server.

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 WSO2-2018-0455

Overview

In the username/password recovery flows, the error messages returned might lead to username harvesting.

Description

Through username enumeration, an attacker would be able to identify the valid user accounts in the system.

Severity

Medium

Impact

Upon gathering the valid user account names, an attacker would then be able to plan other attacks on the identified targets.

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 WSO2-2018-0459

Overview

Adding capability to Disable weak ciphers for Thrift AuthenticationService (port 10711).

Description

When "TLS" is configured as the SSL protocol, the TLS and the default ciphers get enabled without considering the strength of the ciphers. Using an insufficient length for a key in an encryption /decryption algorithm opens up the possibility for security risk.

Severity

Low

Impact

Using Weak ciphers in TLS can make the system vulnerable to attacks such as the Logjam attack (Man-in-the-Middle attack) on Diffie-Hellman key exchange.

Solution

The recommended solution to disable the weak ciphers is to apply the provided patch/update to the respective 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 WSO2-2018-0461

Overview

Potential Cross-Site Scripting (XSS) vulnerabilities have been identified in the Identity Provider Management UI

Description

The XSS vulnerability is detected in the idp-mgt-edit.jsp

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.

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 WSO2-2018-0473

Overview

Second factor of an authentication can be by passed during a double submit event

Description

In an event of double submit to the authentication endpoint, user's can bypass the second factor of the authentication in some specific browsers

Severity

Medium

Impact

Using a client side modifications, an attacker can successfully bypass the second factor of the authentication.

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

-

Security Advisory WSO2-2018-0488

Overview

A vulnerability has been detected in authentication framework which leads the invalidated users to keep accessing applications which are already authenticated.

Description

Even after invalidating a user by deleting, locking or disabling the account, some session caches do not get invalidated properly. Therefore, a malicious user may be able to access the previously logged in applications until the session or remember me expiry is reached, even after removing the account from the server.

Severity

Low

Impact

By exploiting the vulnerability an attacker could access resources which he or she is no longer supposed to access.

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 WSO2-2018-0492

Overview

Improper Authentication and Authorization vulnerability has been identified in SCIM API in WSO2 Identity Server.

Description

By obtaining a certificate from a trusted certificate authority, it is possible to bypass authorization if the root certificate authority used to sign is available in client truststore.

Severity

High

Impact

Upon successful exploitation of this vulnerability, an unauthorizaed user would be be able to invoke the SCIM API.

Solution

The recommended solution is to apply relevant security patches/updates.

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 WSO2-2018-0517

Overview

Make the sigining algorithm of SAML SSO and SLO requests configurable.

Description

When signing a SAML Single Sign On (SSO) or Single Logout (SLO) request, WSO2 server currently uses SHA-1 hashing and it is not configurable. With this fix, the signing algorithm is made configurable and encouraged to use SHA-256.

Severity

Low

Impact

When using SHA-1 hashing, since it is proven to have collisions, an attacker might be able to forge a signed SAML SSO/SLO request which then can be used to gain the SAML authentication response /assertion or forcefully logout the user.

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

-

Security Advisory WSO2-2018-0537

Overview

Upgrade the BouncyCastle version to 1.60 to mitigate reported security vulnerablilities.

Description

Some security vulnerabilities have been identified in BouncyCastle versions released prior to 1.60.

Severity

Low

Impact

The WSO2 products are exposed to known vulnerabilities of BouncyCastle versions prior to 1.60.

Solution

The recommended solution is to apply the provided patch/update to the affected versions of the products. The patch/update is to upgrade the BouncyCastle dependency to version 1.60.

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 WSO2-2019-0545

Overview

A potential Open Redirect vulnerability has been identified in account recovery and self-sign up flow.

Description

Open Redirect vulnerability is dicovered during accout recovery and self-sign up flow, where the page will be redirected directly to the callback URL in the request which can be a malicious one.

Severity

Medium

Impact

An attacker can modify the query parameter value to a URL value of a malicious site,and trick a user to invoke the modified URL. This redirects the user to the malicious site and the attacker may successfully launch a phishing scam and steal user credentials or other sensitive information.

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 in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Credits

-

Security Advisory WSO2-2019-0572

Overview

Upgrade the Open SAML version to 2.6.6 to mitigate reported security vulnerablilities in lower versions.

Description

This patch/update upgrades the OpenSAML library to 2.6.6 in order to address the security vulnerability reported in CVE-2015-1796.

Severity

Medium

Impact

The PKIX trust engines in OpenSAML Java (OpenSAML-J) versions prior to 2.6.5 trust candidate X. 509 credentials when no trusted names are available for the entityID, which allows remote attackers to impersonate an entity via a certificate issued by a shibmd:KeyAuthority trust anchor.

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 WSO2-2019-0577

Overview

Upgrade the commons-codec dependency version to 1.10 to mitigate reported security vulnerablilities in lower versions.

Description

This patch/update upgrades the commons-codec dependency version to 1.10 in order to address a security vulnerability base64 encode flow.

Severity

Medium

Impact

Base64 encode() method is no longer thread-safe in Apache Commons Codec before version 1.7, which might disclose the wrong data or allow an attacker to change non-private fields.

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 WSO2-2019-0582

Overview

[Remove Groovy third party jar which is packed with human task feature of WSO2 products.]

Description

[This patch/update removes the Groovy third party library in order to address the security vulnerability reported in CVE-2016-6814.]

Severity

[Low]

Impact

[When an application with Groovy on classpath uses standard Java serialization mechanisms, e.g. to communicate between servers or to store local data, it is possible for an attacker to bake a special serialized object that will execute code directly when deserialized.]

Solution

[The recommended solution is to apply the provided patch/update to the affected versions of the products. The patch/update is to remove the Groovy third party library from plugins in WSO2 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

[-]

Updated Files

- dbscripts/identity/db2.sql
- dbscripts/identity/h2.sql
- dbscripts/identity/mssql.sql
- dbscripts/identity/mysql-5.7.sql
- dbscripts/identity/mysql.sql
- dbscripts/identity/oracle.sql
- dbscripts/identity/oracle_rac.sql
- dbscripts/identity/postgresql.sql
- lib/org.wso2.ciphertool-1.0.0-wso2v3.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.basicauth-5.3.7.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.samlsso-5.1.12.jar
- repository/components/dropins/org.wso2.carbon.identity.oauth2.token.handler.clientauth.tlswithidsecret-1.0.7.jar
- repository/components/plugins/axiom_1.2.11.wso2v11.jar
- repository/components/plugins/axis2_1.6.1.wso2v23.jar
- repository/components/plugins/bcprov-jdk15on_1.52.0.wso2v1.jar
- repository/components/plugins/commons-codec_1.4.0.wso2v1.jar
- repository/components/plugins/commons-fileupload_1.3.2.wso2v1.jar
- repository/components/plugins/geronimo-kernel_2.0.1.wso2v1.jar
- repository/components/plugins/javax.cache.wso2_4.4.26.jar
- repository/components/plugins/opensaml_2.6.4.wso2v3.jar
- repository/components/plugins/org.jaggeryjs.hostobjects.file_0.12.6.jar
- repository/components/plugins/org.jaggeryjs.hostobjects.xhr_0.12.6.jar
- repository/components/plugins/org.wso2.carbon.application.deployer_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.consent.mgt.core_1.0.50.jar
- repository/components/plugins/org.wso2.carbon.consent.mgt.ui_1.0.50.jar
- repository/components/plugins/org.wso2.carbon.core_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.identity.application.authentication.framework_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.application.common_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.application.mgt.stub_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.application.mgt.ui_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.application.mgt_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.auth.service_1.1.16.jar
- repository/components/plugins/org.wso2.carbon.identity.authenticator.saml2.sso.common_5.2.6.jar
- repository/components/plugins/org.wso2.carbon.identity.authenticator.saml2.sso.ui_5.2.6.jar
- repository/components/plugins/org.wso2.carbon.identity.authenticator.saml2.sso_5.2.6.jar
- repository/components/plugins/org.wso2.carbon.identity.authenticator.thrift_5.11.148.jar

- repository/components/plugins/org.wso2.carbon.identity.authz.service_1.1.16.jar
- repository/components/plugins/org.wso2.carbon.identity.base_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.captcha_1.1.7.jar
- repository/components/plugins/org.wso2.carbon.identity.core_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.data.publisher.oauth_1.0.3.jar
- repository/components/plugins/org.wso2.carbon.identity.entitlement_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.governance_1.1.7.jar
- repository/components/plugins/org.wso2.carbon.identity.idp.metadata.saml2_1.0.5.jar
- repository/components/plugins/org.wso2.carbon.identity.mgt_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.oauth.common_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.oauth.dcr_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.oauth.stub_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.oauth.ui_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.oauth_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.oidc.session_5.6.63.jar
- repository/components/plugins/org.wso2.carbon.identity.provisioning_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.recovery.ui_1.1.7.jar
- repository/components/plugins/org.wso2.carbon.identity.recovery_1.1.7.jar
- repository/components/plugins/org.wso2.carbon.identity.scim.common_5.3.22.jar
- repository/components/plugins/org.wso2.carbon.identity.scim2.common_1.1.19.jar
- repository/components/plugins/org.wso2.carbon.identity.sso.saml.ui_5.4.6.jar
- repository/components/plugins/org.wso2.carbon.identity.sso.saml_5.4.6.jar
- repository/components/plugins/org.wso2.carbon.identity.sts.passive_5.2.16.jar
- repository/components/plugins/org.wso2.carbon.identity.user.profile_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.identity.user.store.configuration.ui_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.idp.mgt.stub_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.idp.mgt.ui_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.idp.mgt_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.logging.service_4.6.21.jar
- repository/components/plugins/org.wso2.carbon.ndatasource.core_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.ndatasource.rdbms_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.registry.resource.ui_4.6.28.jar
- repository/components/plugins/org.wso2.carbon.sts_5.2.16.jar
- repository/components/plugins/org.wso2.carbon.tenant.keystore.mgt_4.6.11.jar
- repository/components/plugins/org.wso2.carbon.tenant.mgt_4.6.11.jar
- repository/components/plugins/org.wso2.carbon.tomcat.ext_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.tomcat_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.user.api_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.user.core_4.4.26.jar
- repository/components/plugins/org.wso2.carbon.user.mgt_5.11.148.jar
- repository/components/plugins/org.wso2.carbon.utils_4.4.26.jar
- repository/components/plugins/org.wso2.charon3.core_3.0.7.jar
- repository/components/plugins/rampart-core_1.6.1.wso2v26.jar
- repository/components/plugins/rampart-trust_1.6.1.wso2v26.jar
- repository/components/plugins/siddhi-core_3.2.3.jar
- repository/components/tools/forget-me/conf/log-config/apim-patterns.xml
- repository/components/tools/forget-me/conf/log-config/is-patterns.xml
- repository/conf/claim-config.xml
- repository/conf/identity/identity.xml
- repository/deployment/server/jaggeryapps/dashboard/css/bootstrap.min.css
- repository/deployment/server/jaggeryapps/dashboard/css/navigation.css
- repository/deployment/server/jaggeryapps/dashboard/css/portal-dashboard-designer.css
- repository/deployment/server/jaggeryapps/dashboard/css/styles.css
- repository/deployment/server/jaggeryapps/dashboard/index.jag
- repository/deployment/server/jaggeryapps/dashboard/js/bootstrap.min.js
- repository/deployment/server/jaggeryapps/dashboard/js/navigation.js
- repository/deployment/server/jaggeryapps/dashboard/js/portal-dashboard-designer.js
- repository/deployment/server/webapps/accountrecoveryendpoint.war
- repository/deployment/server/webapps/api#identity#consent-mgt#v1.0.war
- repository/deployment/server/webapps/api#identity#entitlement.war
- repository/deployment/server/webapps/api#identity#oauth2#dcr#v1.0.war
- repository/deployment/server/webapps/api#identity#oauth2#v1.0.war
- repository/deployment/server/webapps/api#identity#recovery#v0.9.war
- repository/deployment/server/webapps/api#identity#user#v1.0.war

- repository/deployment/server/webapps/authenticationendpoint.war
- repository/deployment/server/webapps/emailotpauthenticationendpoint.war
- repository/deployment/server/webapps/forgetme#v1.0.war
- repository/deployment/server/webapps/oauth2.war
- repository/deployment/server/webapps/scim2.war
- repository/deployment/server/webapps/shindig.war
- repository/deployment/server/webapps/smsotpauthenticationendpoint.war
- repository/deployment/server/webapps/wso2.war
- repository/deployment/server/webapps/x509certificateauthenticationendpoint.war

Added Files

- bin/update_darwin
- bin/update_linux
- repository/components/dropins/bcpkix-jdk15on-1.60.0.wso2v1.jar
- repository/components/dropins/org.wso2.carbon.crypto.api-1.0.1.jar
- repository/components/dropins/org.wso2.carbon.crypto.impl-1.0.1.jar
- repository/components/dropins/org.wso2.carbon.crypto.provider-1.0.1.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.emailotp.connector-2.0.12.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.office365.connector-1.0.4.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.office365.connector-1.0.5.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.smsotp.connector-2.0.12.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.smsotp.connector-2.0.15.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.x509Certificate.connector-2.0.6.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.x509Certificate.connector-2.0.8.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.x509Certificate.validation-1.0.2.jar
- repository/components/dropins/org.wso2.carbon.healthcheck.api.core-1.0.0.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.fido-5.1.14.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.oidc-5.1.16.jar
- repository/components/dropins/org.wso2.carbon.identity.oauth2.grant.jwt-1.0.11.jar
- repository/components/dropins/org.wso2.carbon.identity.oauth2.token.handler.clientauth.tlswithidsecret-1.0.7.jar
- repository/components/tools/forget-me/ext/user-store/conf/config.json
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/cm-receipt.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/cm-receipt.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/fido-device-store.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-associated-id.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-identity-meta-data.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-identity-meta-data.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-identity-user-data.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-identity-user-data.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth-consumer-apps.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth1a-access-token.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth1a-access-token.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth1a-request-token.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth1a-request-token.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth2-accesstoken.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-oauth2-authorization-code.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-openid-remeber-me.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-openid-remeber-me.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-openid-users-rps.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-openid-users-rps.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-password-history-data.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-recovery-data.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-saml2-assertion-store.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-saml2-assertion-store.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-thrift-session.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-thrift-session.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/idn-user-account-association.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/sp-app.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/um-system-user.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/um-system-user.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/wf-bps-profile.sql

- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/wf-bps-profile.sql.properties
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/wf-request.sql
- repository/components/tools/forget-me/ext/user-store/conf/sql/identity/wf-request.sql.properties
- repository/components/tools/forget-me/lib/axiom_1.2.11.wso2v11.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.base_4.4.26.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.logging_4.4.26.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.privacy.forgetme.userstore-1.1.15.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.user.api_4.4.26.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.user.core_4.4.26.jar
- repository/components/tools/forget-me/lib/org.wso2.carbon.utils_4.4.26.jar
- repository/components/tools/forget-me/lib/org.wso2.securevault_1.0.0.wso2v2.jar
- repository/components/tools/forget-me/lib/xercesImpl-2.8.1.wso2v2.jar
- repository/conf/health-check-config.xml
- repository/conf/security/certificate-validation.xml
- repository/deployment/server/jaggeryapps/dashboard/js/jquery-2.1.0.min.js
- repository/deployment/server/webapps/api#health-check#v1.0.war
- repository/deployment/server/webapps/forgetme#v1.0.war
- updates/product.txt

Removed Files

- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.emailotp.connector-2.0.9.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.office365.connector-1.0.2.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.office365.connector-1.0.4.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.smsotp.connector-2.0.11.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.smsotp.connector-2.0.12.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.x509Certificate.connector-2.0.4.jar
- repository/components/dropins/org.wso2.carbon.extension.identity.authenticator.x509Certificate.connector-2.0.6.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.fido-5.1.11.jar
- repository/components/dropins/org.wso2.carbon.identity.application.authenticator.oidc-5.1.15.jar
- repository/components/dropins/org.wso2.carbon.identity.oauth2.grant.jwt-1.0.10.jar
- repository/components/plugins/groovy-all_2.3.9.jar