EEI-CVE-2022-29464-Recovery

If a malicious actor gains access to the EEI server(s), this document outlines the steps to be completed to fully recover from the breach.

EEI Compromised Server Recovery

APRIL 2022

Tom O'Neill, Senior Consultant

CONTENTS

EEI COMPROMISED SERVER RECOVERY

Overview

If a malicious actor gains access to the EEI server(s) the following steps should be completed to fully recover from the breach:

- ❑ Change the Carbon Console Password
- ❑ Change the EEI Database Passwords
- ❑ Change the LDAP Connection Passwords
- ❑ Change the SAML Signing Certificate

These steps should only be completed after restoring to a backup image, moving to a new server(s) or fully removing any malware located on the EEI servers.

Change the Carbon Console Password

The Carbon Console is a powerful tool with the ability to manage the IdP and view the directory of users. The credentials are stored in plaintext in multiple files and should be changed if the server is ever compromised.

1. Change the password in the underlying PRIMARY userstore
    a. The PRIMARY userstore can be identified by reviewing the following settings
        i. eis.userstore.type
        ii. eis.userstore.ConnectionURL
        iii. eis.userstore.ConnectionName
        iv. eis.userstore.UserSearchBase
    b. The admin account can be identified by reviewing the following settings
        i. eis.admin.username
        ii. eis.admin.password
2. Update the credentials stored in the $EIS_HOME/config/eis_config.properties
    a. eis.admin.username
    b. eis.admin.password
3. From the 'wso2is-5.x.0' directory, run the 'update-user-mgt-xml' target to push the changes to user-mgt.xml
    a. apache-ant/bin/ant update-user-mgt-xml -buildfile config/build.xml
4. Restart the application

Change the EEI Database Passwords

EEI stores configuration information and transient session data in the database. The database connection is defined in eis_config.properties and then an Apache Ant command is propagate the values to the master-datasources.xml file.

1. Shut down the application
2. Change the password in the underlying database (Oracle, MySQL, SQL Server)
3. Update the credentials listed in the $EIS_HOME/config/eis_config.properties file
    a. eis.database.username
    b. eis.database.password
    c. eis.cluster.registry.username
    d. eis.cluster.registry.password
    e. eis.cluster.identity.username
    f. eis.cluster.identity.password
4. From the 'wso2is-5.x.0' directory, run the 'update-datasources-xml' target to push the changes to master-datasources.xml
    a. apache-ant/bin/ant update-datasources-xml -buildfile config/build.xml
5. Start the application

Change the LDAP Connection Passwords

LDAP credentials can be configured for connections in two places:

- Primary Userstore
- Secondary Userstores

Updating the Primary Userstore

The Primary userstore is the LDAP connection configured in the eis_config.properties file. The values are then propagated out to the $EIS_HOME/repository/conf/user-mgt.xml file by running an Apache Ant command.

1. Stop the application
2. Change the password in the underlying PRIMARY userstore
3. Change the credentials listed in the $EIS_HOME/config/eis_config.properties file
    a. eis.userstore.ConnectionName
    b. eis.userstore.ConnectionPassword
4. From the 'wso2is-5.x.0' directory, run the 'update-user-mgt-xml' target to push the changes to user-mgt.xml
    a. apache-ant/bin/ant update-user-mgt-xml -buildfile config/build.xml
5. Start the application

Updating Secondary Userstores

Secondary LDAP connections are typically configured through the Carbon Console and get stored as XML files on the filesystem. The XML documents can be edited directly but updating the configuration through the Carbon Console is best practice.

The secondary userstore XML files can be found in the following directory:
$EIS_HOME/repository/deployment/server/userstores

NOTE: If the entry was created through the UI, the password may be encrypted.

NOTE: If the installation is clustered, then the files will need to be synchronized between nodes.

NOTE: Changes to secondary userstores do not require a restart.

Change the SAML Signing Certificate

The SAML signing certificate is used to secure SAML 2.0 transactions and should be replaced if there is a chance that the public/private keypair was compromised.

Please reach out to a SIG consultant to discuss the approach and steps for replacing the SAML signing certificate in your environment(s).

This part is a bit more involved and may require coordinating updates with application administrators and third-party vendors.

NOTE: If your institution has Identity Providers configured that use SAML 2.0 for SSO, the change will need to be coordinated with the IdP administrator to make sure SSO does not break.

NOTE: If your institution has Service Provider applications that use SAML 2.0 for SSO, the change will need to be coordinated with the SP application administrator to make sure SSO does not break.

NOTE: If your institution has Secondary Userstores configured, it is likely that the passwords are encrypted using the same keypair and passwords must be entered again to avoid breaking LDAP connections.

1. Review the considerations above, identify any impacted applications and develop a plan to update the certificate with minimal downtime

2. Identify the keystore that the application is configured to use by reviewing the following settings in the eis_config.properties file:
    a. eis.keystore.location
    b. eis.keystore.password
    c. eis.keystore.private.key.alias
    d. eis.keystore.private.key.password

3. Create a backup copy of the keystore referenced in the 'eis.keystore.location' property

4. Create a working copy of the keystore referenced in the 'eis.keystore.location' property

   NOTE: Steps 5, 6 and 7 should be run against the working copy of the EEI keystore

5. Run the keytool delete command to delete the current entry under the alias 'wso2carbon'
   a. keytool -delete -alias wso2carbon -keystore wso2carbon.jks

6. Run the keytool genkeypair command to create a new public/private keypair that expires in 5 years.
   a. keytool -genkeypair -keyalg RSA -alias wso2carbon -dname "CN=sso.school.edu,O=Organization,L=Locality,ST=State,C=Country" -validity 1825 -keysize 2048 -keystore wso2carbon.jks

7. Run the keytool command to output the public certificate, saving the contents to a text file.
   a. keytool -list -rfc -alias wso2carbon -keystore wso2carbon.jks

8. Retrieve the current metadata by accessing the following URL (EEI 5.3 and higher).
   a. https://sso.school.edu/identity/metadata/saml2

9. Create a copy of the metadata returned and replace the certificate in the `X509Certificate` tag with the output from Step 7:
   a. This will be the new EEI IdP metadata when the next step is completed. Share this document in advance with Service/Identity Providers but make sure to communicate clearly when step 9 is expected to be done.
   b. If the change is not coordinated, SSO will likely break until both parties are configured to be using the same certificates.

10. When ready for cutover, copy the modified, working copy of the keystore back to the 'eis.keystore.location'

11. Restart the application.