Closed Opened 1 week ago by muffinx

Secure-Data-Manager OrientDB Username same as Password

Dear E-Voting PIT Team

Inside the secure-data-manager there is an implementation of a orient database.

Now inside this class, we can see that the default username and default password are the same for the DatabaseManager.

/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-services/src/main/java/com/scytl/products/ov/sdm/infrastructure/DatabaseManagerFactory.java

```
public interface DatabaseManagerFactory {
    /**
     * The default user name.
     */
    String DEFAULT_USERNAME = OUser.ADMIN;

    /**
     * The default password.
     */
    String DEFAULT_PASSWORD = OUser.ADMIN;

    /**
     * Creates a new database manager for given URL and the default user. This
     * is a shortcut for
     * {@code newDatabaseManager(url, DEFAULT_USERNAME, DEFAULT_PASSWORD)}.
     *
     * @param url
     *            the URL
     * @return the database manager
     */
    DatabaseManager newDatabaseManager(String url);

    /**
     * Creates a new database manager for given URL and user.
     *
     * @param url
     *            the URL
     * @param username
     *            the user name
     * @param password
     *            the password
     * @return the database manager
     */
    DatabaseManager newDatabaseManager(String url, String username,
            String password);
}
```

We can also see that there are two ways to call newDatabaseManager(), one by just passing one parameter (url), or three parameters (url, username and password).

Now inside the implementation we found that when calling with one parameter (url), the default username and password will be used:

```
public final class DatabaseManagerFactoryImpl
        implements DatabaseManagerFactory {

    @Override
    public DatabaseManager newDatabaseManager(final String url) {
        return newDatabaseManager(url, DEFAULT_USERNAME, DEFAULT_PASSWORD);
    }

    @Override
    public DatabaseManager newDatabaseManager(final String url,
            final String username, final String password) {
```

```
        return new DatabaseManagerImpl(url, username, password);
    }
}
```

When searching for newDatabaseManager() calls, we could only find call which pass one parameter (a url):

```
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-ws-rest/src/main/java/c
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-db-utils/src/main/java/
```

Now whatever the username is, the password is the same for the orient database. For example if the username is "admin", so the password is also "admin".

So this is a huge issue, since someone could possibly find out the username pretty simple.

Thank you very much for reading my report.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi

Swisspost @swisspost added (In Progress) (topic: general) labels 1 week ago

Swisspost @swisspost · 1 week ago Maintainer

Hi Anthony,

Thank you for your input. We will verify this and get back to you.

Kind regards

Swisspost @swisspost · 1 week ago Maintainer

Hi Anthony,

First of all, thank you, muffinx for all the time and effort you put into analyzing the code. Some of your observations are very valuable for us future improvements of the product. Regarding this point, we will provide you an answer similiar to your last observation. One has to make a distinction between components running in a network (where proper authentication is absolutely crucial) and stand alone applications, running on dedicated hardware on the canton's premises, where authentication is more or less implicit (one needs physical access + username / password of the machines). OrientDB is part of the SDM standalone application and therefore, the authentication between the SDM and orientDB is more or less superfluous.

I hope this helps.

Kind regards

Swisspost @swisspost closed 1 week ago

Swisspost @swisspost removed (In Progress) label 1 day ago

Swisspost @swisspost made the issue visible to everyone 1 day ago