MWR LABS

Security Advisory

# Studiometry – Insecure Password Storage

## 2016-07-25

| | |
|---|---|
| Software | Studiometry |
| Affected Versions | 12.5.6 – Windows version<br>12.6 – Windows version<br>(only two versions tested) |
| CVE Reference | N/A |
| Author | Bryan Schmidt |
| Severity | High |
| Vendor | Oranged Software |
| Vendor Response | Patch Issued |

## Description:

Studiometry is a project and client management tool that is directed at small business. The tool comes in several forms with both a Windows and Mac OSX implementation. Additionally, cloud services are provided as well as an iOS mobile application. The Windows version of the application was tested but the advisory could affect the iOS and Mac OSX implementations. The configuration was that of a self-administered Studiometry server that a small business would be likely to use.

It was discovered that Studiometry stores user account passwords in encoded base64 format on both the server and its clients.

## Impact:

An attacker that has obtained access to a Studiometry database stored either on the server or one of its clients could easily decode all the users' passwords for the application.

## Cause:

Insecure design and database management.

## Interim Workaround:

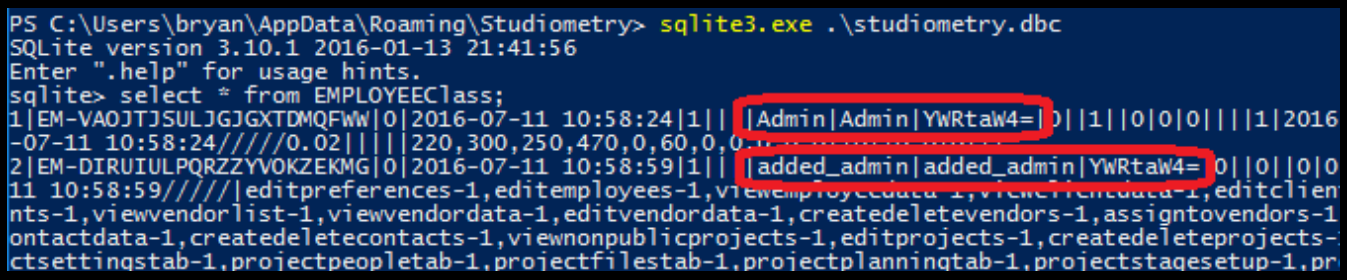
Ensure the Studiometry database is stored in a secure location on both clients and the Studiometry server. Additionally, only allow access by trusted employees to the Studiometry server.

## Solution:

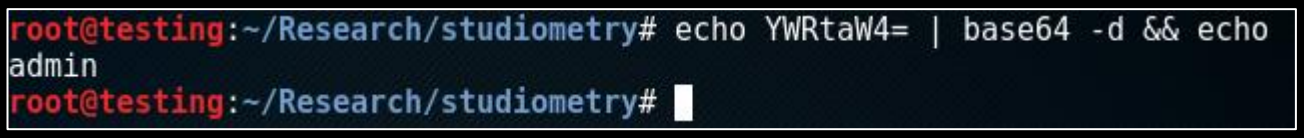
Update to Studiometry 12.6.1.

## Technical details

Studiometry was identified as using SQLite to store the applications data. In the default Windows installation, the application stores the database (studometry.dbc) in the 'AppData' directory within the User directory of the user that installed the application. Due to the nature of SQLite, the contents of the database are stored within an easily accessible text file. Within the database, the account passwords can be seen as stored in a base64 encoded format as depicted in the following screenshot:




When stored in this format, the passwords can easily be decoded using the 'base64' utility provided by default on Kali Linux, as seen in the following screenshot:




## Further Information

http://oranged.net/studiometry/versionhistory/

## Detailed Timeline

| Date | Summary |
|---|---|
| 2016-07-11 | Issue reported to vendor |
| 2016-07-11 | Response received from vendor |
| 2016-07-13 | Vendor provided beta with patches for testing. Vulnerability verified as fixed in beta. |
| 2016-07-14 | Vendor notified MWR that an official patch would be released 2016-07-25. |
| 2016-07-25 | Oranged Software released official patched version 12.6.1 of Studiometry |