PurplePetrus Added SW Version History

1 contributor

89 lines (68 sloc) | 2.44 KB

```
1  ######################################
2  MxCC passwords exposed in MxCC.ini file
3  ######################################
4
5
6  Software: Mobotix Control Center (MxCC)
7  Version: 2.5.4.5 and before
8
9  Summary:
10 --------
11
12 In the config file created by MxCC, when saving the config, the passwords are stored in base64 for
13 This format can easily be reversed and passwords become visible in cleartext.
14
15 It concerns following passwords:
16
17 - Camera passwords
18 - MxCC Users passwords
19 - network share passwords
20
21 Tested in Version 2.5.4.5
22
23
24 Test case:
25 ----------
26
27 *setup*
28
29 Created config with 2 users
```

```
one admin user and one regular user.
admin user with password: supersecretpassword
regular user with password: myownpassword

the config was saved and found in the appdata directory of the user.

extract of config file with user info:
--------------------------------------

* start example *

[UsersnGroups]
Group\size=2
Group\1\GroupID=0
Group\1\Name=administrators
Group\1\Comment=
Group\1\User\size=1
Group\1\User\1\UserID=0
Group\1\User\1\Name=admin
Group\1\User\1\FullName=admin
Group\1\User\1\Comment=
Group\1\User\1\Password="@ByteArray(c3VwZXJzZWNyZXRwYXNzd29yZA==)"
Group\1\User\1\GroupID=0
Group\1\User\1\AutoLogOn=0
Group\2\GroupID=1
Group\2\Name=users
Group\2\Comment=
Group\2\User\size=1
Group\2\User\1\UserID=1
Group\2\User\1\Name=user
Group\2\User\1\FullName=
Group\2\User\1\Comment=
Group\2\User\1\Password="@ByteArray(bXlvd25wYXNzd29yZA==)"
Group\2\User\1\GroupID=1
Group\2\User\1\AutoLogOn=0
Obscure=true
HighestUserID=1
HighestGroupID=1

* end of example *


As we can see in the @ByteArray we can find a base64 data string.
if we run this string in a base64 decoder we can recreate the passwords in plain text.
This for all passwords in the file.

This file is often backed up on a different location in order to recover a config when lost.
This file is also present on the workstation in order to load the config.

```

```
If this file is taken or accessed by an unauthorized person/process, this person or process can re
- all users in MxCC
- all camera login credentials
- credentials for access to share location if used for remote storage.

This could allow for practically any user with access to this workstation and access to the MxCC a
Which can result in.
-       Unauthorized access to Camera devices
-       Privilige escalation in the context of the application MxCC
-       Unauthorized access to recordings
-       Unauthorized acces to networkshares
```