Technical Document

Improper Access Control Vulnerability in MicroSCADA Pro SYS600 9.x

ABBVU-PGGA-33888

Notice

Products

MicroSCADA Pro SYS600 9.3

MicroSCADA Pro SYS600 9.3 FP3

MicroSCADA Pro SYS600 9.4

MicroSCADA Pro SYS600 9.4 FP1

MicroSCADA Pro SYS600 9.4 FP2

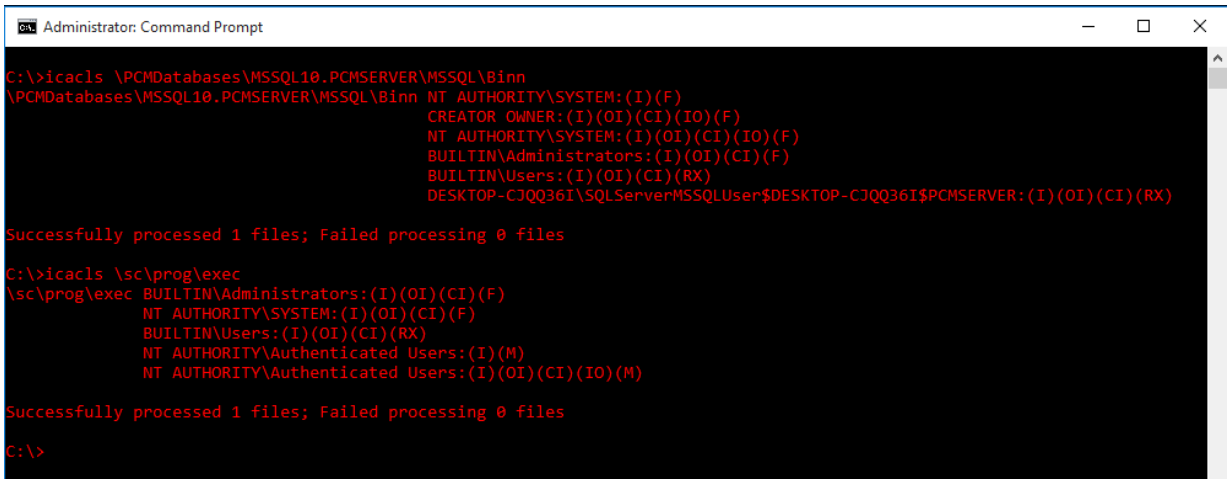
Description

To resolve above mentioned improper access control vulnerability, file system permissions needs to be changed in SYS600 installation directory.

Before fixing, enumerate all non-admin Windows user accounts in the server (Command Prompt: net localgroup users) and document those. Specifically, pay attention to Windows user accounts used by utility operators.

Verify that vulnerability exists

Because the vulnerability is in Windows file system permissions, there might be servers that are hardened and may not be vulnerable. To verify if the vulnerability exists run commands shown in the screenshot:



Note that *MSSQL10.PCMSERVER* directory might have different name in some SYS600 versions.

The server is vulnerable, if non-admin Windows users exist in the server and output of icacls contains M (modify), W (write), AD (append data/add subdirectory), WD (write data/add file), or F (full) permissions for built-in Windows user groups:

a) Authenticated Users

b) BUILTIN\Users

It is normal to have RX (read and execute) permissions for Users group. After running the fix, stricter file system permissions are configured for built-in Users and Authenticated Users groups and more permissions are given for specific Windows groups. Note that ScEngineers group will have more permissions to specific product directories although a non-admin user being a member of this group. This gives better protection of the operating system when an engineer can use the product with less privileges (non-admin) and membership of Administrators group is not required for an engineer (full control of operating system).

The original vulnerability report ABB received stated that MS SQL executables have weak file system permissions under PCMDatabases directory. However, in our investigations we have not found this problem. MSSQL\Binn directory is protected as seen in the above screenshot and non-admin users only have RX permission to this directory.

Backup and restore

When modifying the system it is recommended to take a backup. To backup file system permissions (ACL):

1. Open Command Prompt as administrator
2. cd \
3. icacls c:\sc* /save sc_original.acl /T /C

In error situations, to restore original file system permissions:

1. Open Command Prompt as administrator
2. cd \
3. icacls c:\sc\ /restore sc_original.acl /T /C

Fixing the vulnerability

Preparation:

Copy and paste listing at the end of this document to ABBVU-33888-fix.cmd file and copy this file to C:\ root of the affected server.

Fixing:

1. Open Command Prompt as administrator
2. Go to root directory: cd \
3. Run command: ABBVU-33888-fix.cmd c:\sc
4. Add existing non-admin Windows user accounts, which should have access to SYS600, to correct Windows user groups. In below example, myOperator user account is used:

a. Enumerate Windows users groups (net localgroup) to see that there are groups prefixed with ‘Sc’, e.g. ScOperators.

b. Add Windows user accounts used for operators (and other roles) to the correct Windows user group (net localgroup ScOperators myOperator /add). The previous command adds a membership of ScOperators for myOperator user account. Add Windows user accounts used for administrators to ScSysAdmins Windows user group.

Testing:

1. Logout myOperator from Windows and login again

2. Check that myOperator is able to login to Monitor Pro and navigate process displays, open alarm and event lists and do other normal daily operations.

For troubleshooting, see below section.

Troubleshooting

When running the fix, there are some messages that appear to be errors. However, most of these messages can be ignored.

Problem: Local group exists

The output has following lines:

System error 1379 has occurred.

The specified local group already exist.

Solution:

You can ignore this message. Required Windows user groups already exist.

Problem: File or directory does not exist

The output has following lines:

c:\sc\temp: The system cannot find the file specified

Successfully processed 0 files; Failed processing 1 files

…

c:\sc\prog\sa_lib\default_framewindow.ini: The system cannot find the file specified

Successfully processed 0 files; Failed processing 1 files

Solution:

You can ignore this message. In some SYS600 versions file/directory does not exist.

Problem: A subdirectory or file <> already exists

Solution: You can ignore this message

Problem: Access is denied

The output has following lines:

Import Progs ACL to sc…

.\.: Access is denied

Successfully processed 0 files; Failed processing 1 files

Solution:

You can ignore this message. It appears if running the fix twice. You can run ‘icacls c:\sc /reset’ to restore Windows default permissions. Run a fix again and the error message should not appear.

Problem: Operator cannot login to SYS600 Monitor Pro due to permissions or you receive ‘Failed to save layout’ errors

Solution: Assign a membership of ScOperators group to the non-admin Windows user. The non-admin user needs to login again. Note that even though the user is logged in as a Windows administrator, in some machines the operating system does not give administrator privileges unless the user explicitly uses ‘Run as administrators’. Assign a membership of ScSysAdmins for admin user.

Listing. ABBVU-33888-fix.cmd

```
@echo off
echo FIX START
echo Creating Windows groups...
net localgroup ScOperators /add
net localgroup ScEngineers /add
net localgroup ScSysAdmins /add
net localgroup ScViewers /add

set installdir=%1
set aclcopy=progs.acl
setlocal EnableDelayedExpansion
set /a count=0
set caclstool=icacls
set inherit="(OI)(CI)"
set options=/Q /C

echo Modifying file system permissions ACL... This might take several minutes...
echo Export ACL from Progs...
cd /d "%programfiles%"
%caclstool% . /save %installdir%\%aclcopy%
echo Reset file system permissions...
cd /d %installdir%
%caclstool% . /reset /T %options%
echo Import Progs ACL to sc...
%caclstool% . /restore %aclcopy%
del %aclcopy%
```

```
echo Add additional ACL to sc...
%caclstool% %installdir% /grant:r ScSysAdmins:%inherit%F %options%
%caclstool% %installdir% /grant:r ScEngineers:%inherit%F %options%
%caclstool% %installdir%\sa_lib\defaults\misc /grant ScViewers:%inherit%M %options%
%caclstool% %installdir%\sa_lib\defaults\misc /grant ScOperators:%inherit%M %options%
%caclstool% %installdir%\temp /grant ScViewers:%inherit%M %options%
%caclstool% %installdir%\temp /grant ScOperators:%inherit%M %options%
%caclstool% %installdir%\prog\sa_lib\default_FrameWindow.ini /grant ScViewers:W %op-
tions%
%caclstool% %installdir%\prog\sa_lib\default_FrameWindow.ini /grant ScOperators:W %op-
tions%
REM BEGIN: Uncomment below commands for SYS600 9.3 systems
REM %caclstool% %installdir%\prog\sa_lib  /grant ScViewers:M %options%
REM %caclstool% %installdir%\prog\sa_lib /grant ScOperators:M %options%
REM END: Uncomment above commands for SYS600 9.3 systems
for /f "delims=" %%A in ('dir %installdir%\apl /ad /b') do (
    mkdir %installdir%\apl\%%A\PAR
    %caclstool% %installdir%\apl\%%A\PAR /grant ScViewers:%inherit%M %options%
    %caclstool% %installdir%\apl\%%A\PAR /grant ScOperators:%inherit%M %options%
    mkdir %installdir%\apl\%%A\PICT
    %caclstool% %installdir%\apl\%%A\PICT /grant ScViewers:%inherit%M %options%
    %caclstool% %installdir%\apl\%%A\PICT /grant ScOperators:%inherit%M %options%
)
echo FIX END
```

Revisions

03.02.2018	Original document
16.03.2018	Added commands for SYS600 9.3 systems, see “Listing. ABBVU-33888-fix.cmd”. Clarified permissions for non-admin Windows groups, see section Verify that vulnerability exists.
18.11.2020	Fixed the script at the last page. Changed two cd %dir% commands to cd /d %dir% to work correctly also when MicroScada is not installed in c: drive.