ABB DOC ID: 3ADR010586
REVISION: C
DATE: 2020-10-15

CYBER SECURITY ADVISORY

Vulnerabilities in Wibu CodeMeter for Automation Builder

ABBVU-VREP0028-3ADR010586

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Affected Products

Automation Builder (AB) versions 2.3.0.835 and earlier

Vulnerability IDs

ABB ID: ABBVU-VREP0028-3ADR010586

CVE	CVSSv3 Score
CVE-2020-14513	7.5
CVE-2020-14519	8.1
CVE-2020-14509	10.0
CVE-2020-14517	9.4
CVE-2020-16233	7.5
CVE-2020-14515	7.4

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. There are no product updates available yet, but there are other ways to mitigate the vulnerabilities.

An attacker who successfully exploited these vulnerabilities could insert and run arbitrary code.

Update (2020-10-15):

Five of the six vulnerabilities have been closed with Wibu CodeMeter V7.10a. Only CVE-2020-14517 is not closed, but the remote attack vector has been removed.

Wibu CodeMeter V7.10a is available for download from the Wibu website and also integrated into Automation Builder 2.3.0.847. Please see the Workarounds section for details.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2020-14509:

CVSS v3 base score: 10.0 (Critical)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-14519:

CVSS v3 base score of 8.1 (High)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVE-2020-14513

CVSS v3 base score: 7.1 (High)

CVSS v3 Vector: AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2020-14517

A CVSS v3 base score of 9.4 (Critical)

CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVE-2020-16233

CVSS v3.1 base score of 7.5 (High)

CVSS v3.1 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2020-14515

CVSS v3 base score of 7.7 (High)

CVSS v3 vector: AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Recommended immediate actions

ABB is currently investigating this vulnerability in order to provide adequate protection to customers.

There are ways to mitigate the risks by following the instructions in chapters Mitigating Factors and Appendix A: Instructions on how to update CodeMeter for Windows application manually of this document.

Vulnerability Details

A vulnerability exists in the CodeMeter for Windows component included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the node to stop or become inaccessible, allowing the attacker to take control of the product or insert and run arbitrary code.

Mitigating Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include ensuring that protection, control & automation systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. In general protection, control & automation systems should not be used for general business functions which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Block all non-trusted IP communications.

To minimize the risk of exploitation of the CodeMeter vulnerabilities users should take these defensive measures:

- Locate the control system network behind a firewall and separate them from other networks.
- In environments where CodeMeter network license server is not in use, configure firewall to block access to port TCP 22350
- Block anomalous IP traffic by utilizing a combination of firewalls and intrusion prevention systems.
- Disable or block IP tunneling, both IPv6-in-IPv4 or IP-in-IP tunneling.
- Avoid exposure of the devices to the Internet and use secure methods like VPN when accessing them remotely.

Workarounds

ABB has tested the following workarounds. Detailed instructions of some workarounds are in Appendix A of this document.

1. Manually update the CodeMeter for Windows application to version 7.10a or later. This will allow you to continue using your licenses and licensed products.
2. Update (2020-10-15):
   Download and install latest Automation Builder version 2.3.0.847, which is available from the Automation Builder download section of the ABB website:
   https://new.abb.com/plc/automationbuilder/platform/software
3. Manually uninstall CodeMeter for Windows application. Impact of this workaround is that the products this document covers will not run.
4. Disable CodeMeter for Windows from running. Impact of this workaround is that the products this document covers will not run.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could take control of an affected system node or insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by several problems in the CodeMeter for Windows in the mentioned products.

What is the CodeMeter for Windows?

CodeMeter for Windows is used by applications to manage licensing of these applications. The application validates the licensing of the applications on behalf of ABB. CodeMeter is installed as part of products mentioned in this document locally to users' computers.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to insert and run arbitrary code on a target system.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

What happens to my licenses, if I update WIBU CodeMeter Runtime?

Updating the CodeMeter Runtime version does not affect the activated licenses. All licenses that have been available prior to the update will be available after the update without taking any further actions.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Appendix A: Instructions on how to update CodeMeter for Windows application manually

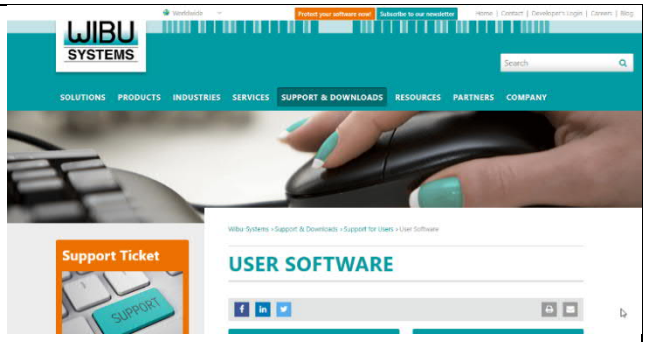
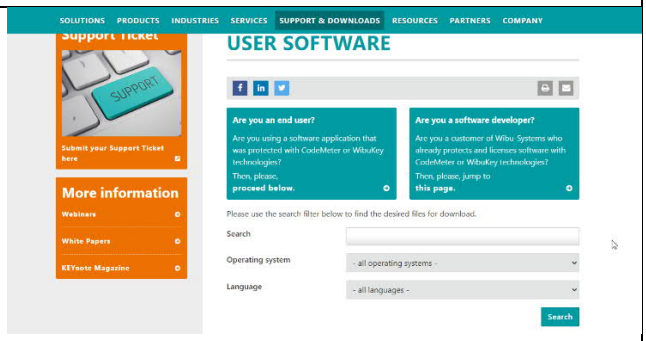
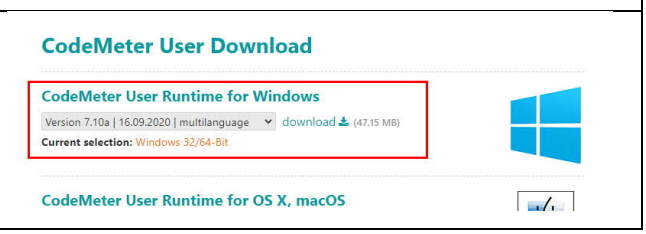
There are different ways to mitigate the risks and this document guides through the easiest ones. Currently the recommended versions for CodeMeter are 7.10a and later.

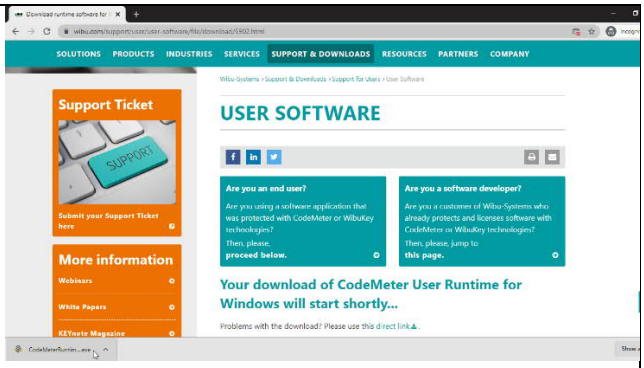
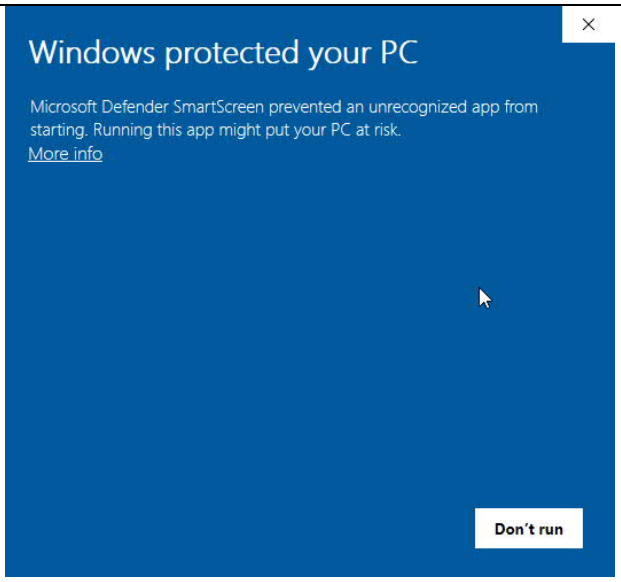
1. Manually install a newer version of CodeMeter

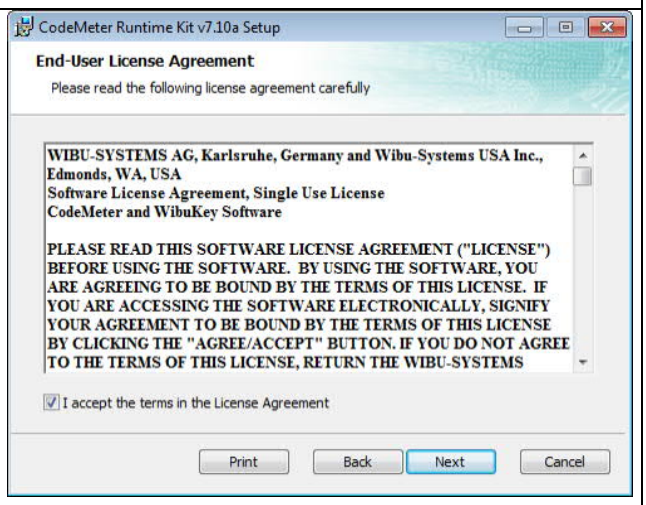
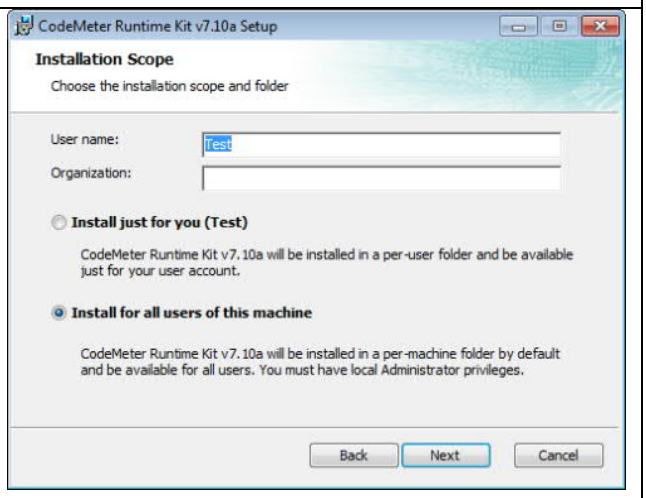
It is possible to download and install a newer version of CodeMeter application to a system to upgrade to a secure version. This version has not been fully tested by ABB and therefore there might be adverse effects with ABB products. If a customer notices changes in the applications' behavior after the update it is requested to report those to ABB.

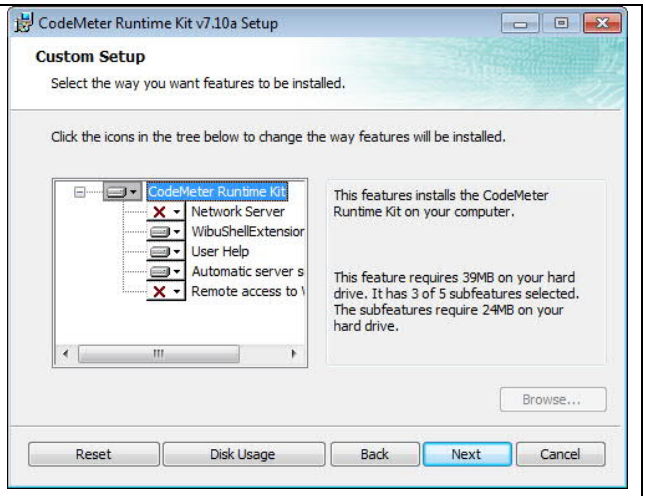
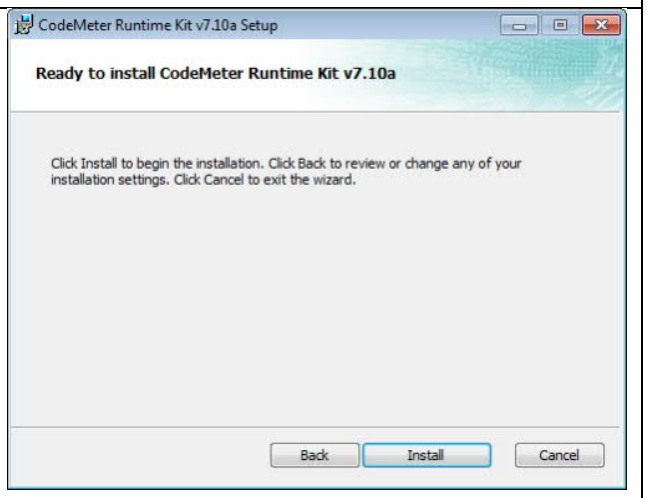
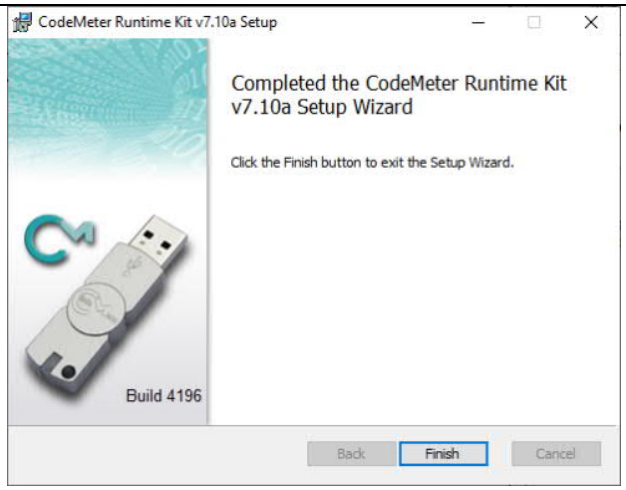
Please notice that updating the CodeMeter Runtime version does not affect the activated licenses. All licenses that have been available prior to the update will be available after the update without taking any further actions.

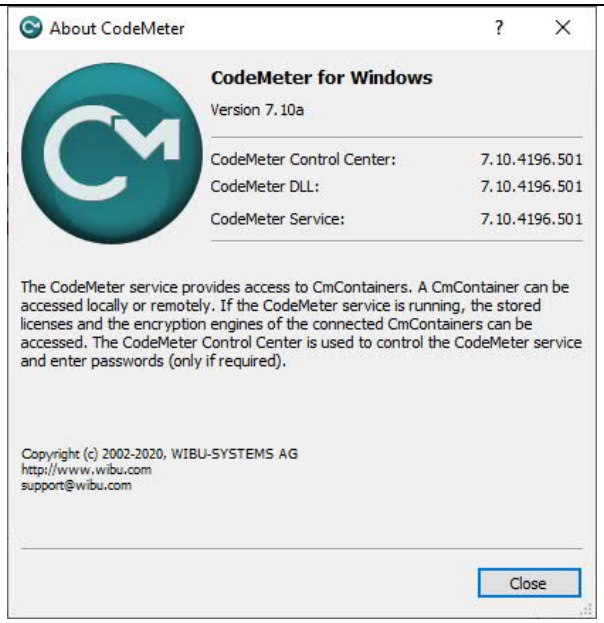
Below are the steps needed to update the CodeMeter application. The steps may vary depending on Windows version and configuration.

1. Use your browser to enter https://www.wibu.com/support/user/user-software.html	
2. Select operating system and language.	
3. Download "CodeMeter User Runtime for Windows".	

4. Once the file has downloaded open the .exe file to start installation. Depending on the browser the location of downloaded file may differ, and you may have to enter Downloads-folder in Windows explorer manually to locate the file.	
5. In case the Windows defender prompts about the risks involved with the application, select “More info” and “Run anyway”. The Microsoft Defender SmartScreen basis the analysis on installation statistics and since the application version is new, at the time of writing this guide the Defender warns about the threat. This dialog does not always appear.	 

6. Click next to start the installation.	
7. Accept End-User License Agreement.	
8. Depending on your installation select the appropriate way to install. It is recommended to install this for all users. This requires local Administrator privileges.	

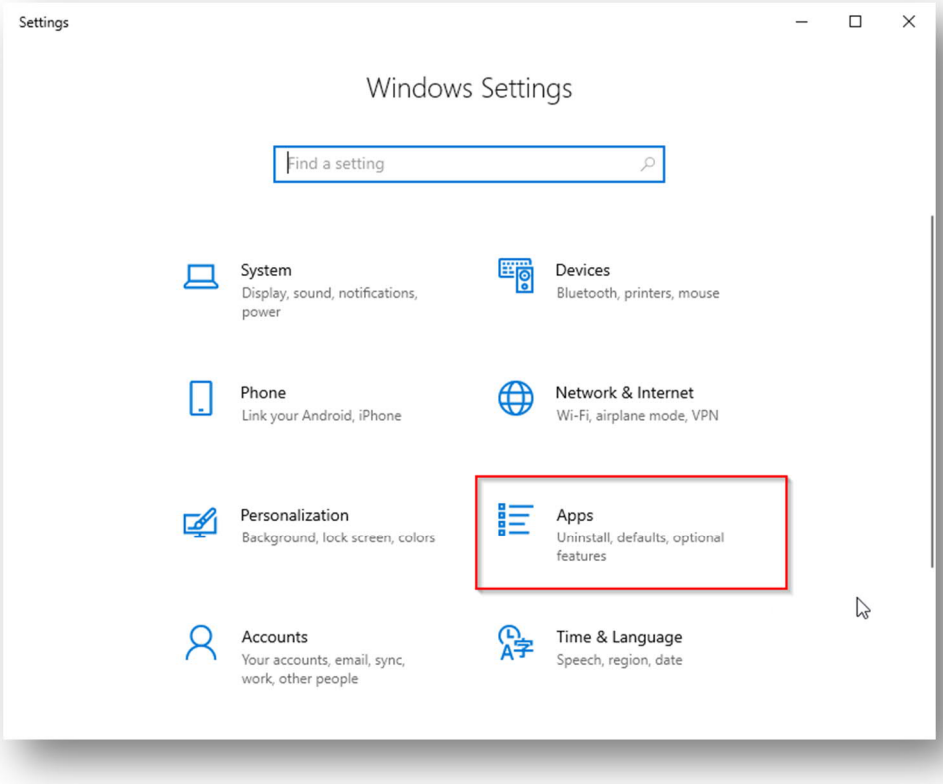
9. Select the components to be installed.	
10. Click Install to start. Installation can take several minutes.	
11. After installation ends, click Finish to close the installer.	

12. From the CodeMeter application Help-menu select About to verify the version in use. Versions 7.10a and later are recommended by ABB at this time.	

2. Uninstall CodeMeter

Following are steps which will allow easily to uninstall CodeMeter. This will result to the ABB applications not being able to run but will secure system. The steps may vary between versions of Windows.

1. In Windows, select Settings from Start-menu.
2. Select Apps



3. Find in the list “CodeMeter Runtime Kit v.6.**” (version number may vary). If the version is 7.10 or later, there is no need to continue.
4. Click the item and select Uninstall.
5. Follow the instructions.

After the CodeMeter has been uninstalled the related vulnerabilities are not present in Windows but the products affected will not run.

3. Stop CodeMeter from running

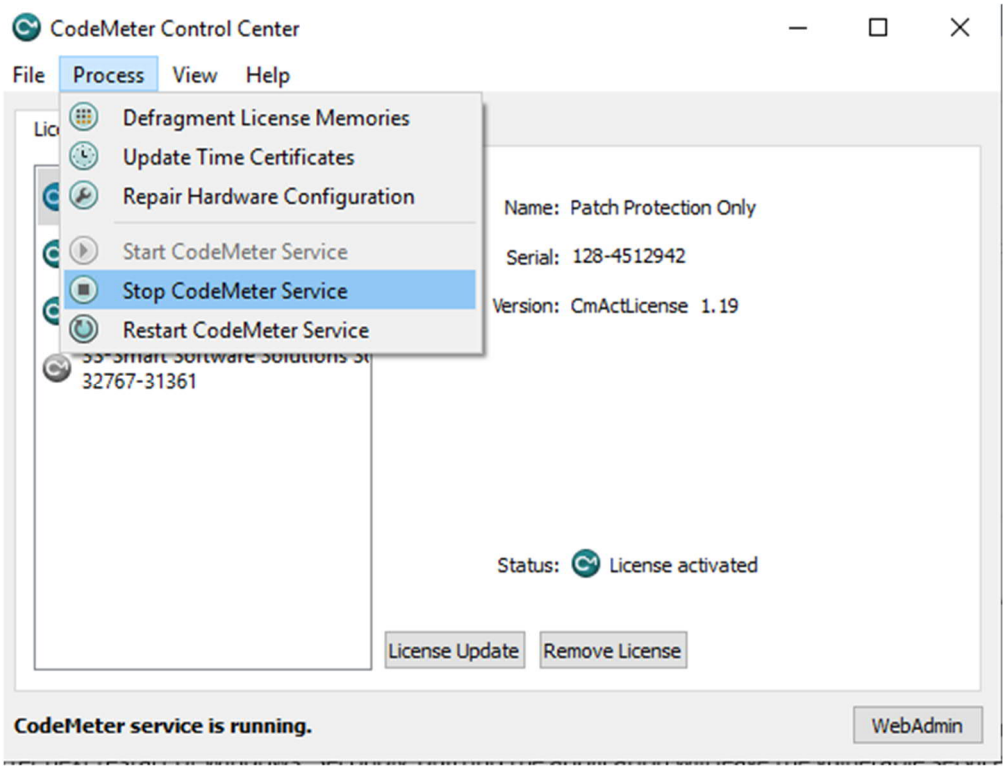
The instructions in this chapter are very temporary and should be taken only as such. Potential reason to use this method is when waiting to install newer version of products affected with this problem.

CodeMeter automatically runs when Windows is started. There is an icon for CodeMeter in the Windows taskbar (normally in the lower left corner of desktop).

With right-clicking the icon, it is possible to quit the application. However, the application will run again after next restart of Windows. Secondly, quitting the application will leave the vulnerable services running in the background.

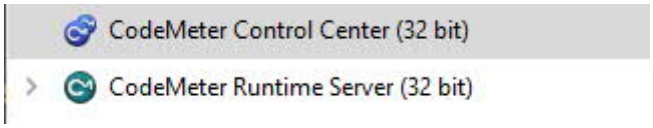
Stop CodeMeter process from running from CodeMeter application

In the CodeMeter application, select “Stop CodeMeter Service”. This will stop the application from running until the next restart of the computer.



Stop CodeMeter from Task Manager

It is possible to go to Windows Task Manager (for example pressing CTRL-ALT-DEL and selecting Task Manager) and selecting End task with right-clicking the Mouse on any entry for CodeMeter.

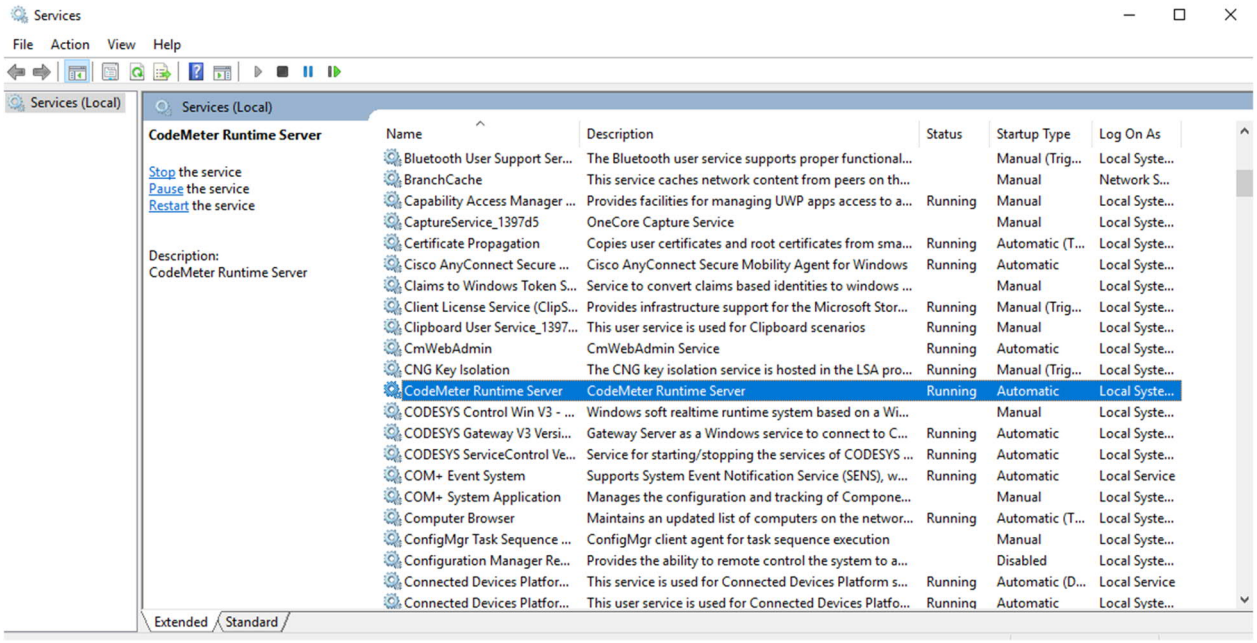


In order to start ABB products using CodeMeter, these processes must be running and therefore when starting these Drives applications will also start CodeMeter. This method will allow restarting the application once Windows is restarted.

Stop CodeMeter running from using Services application in Windows and disable running when Windows is restarted

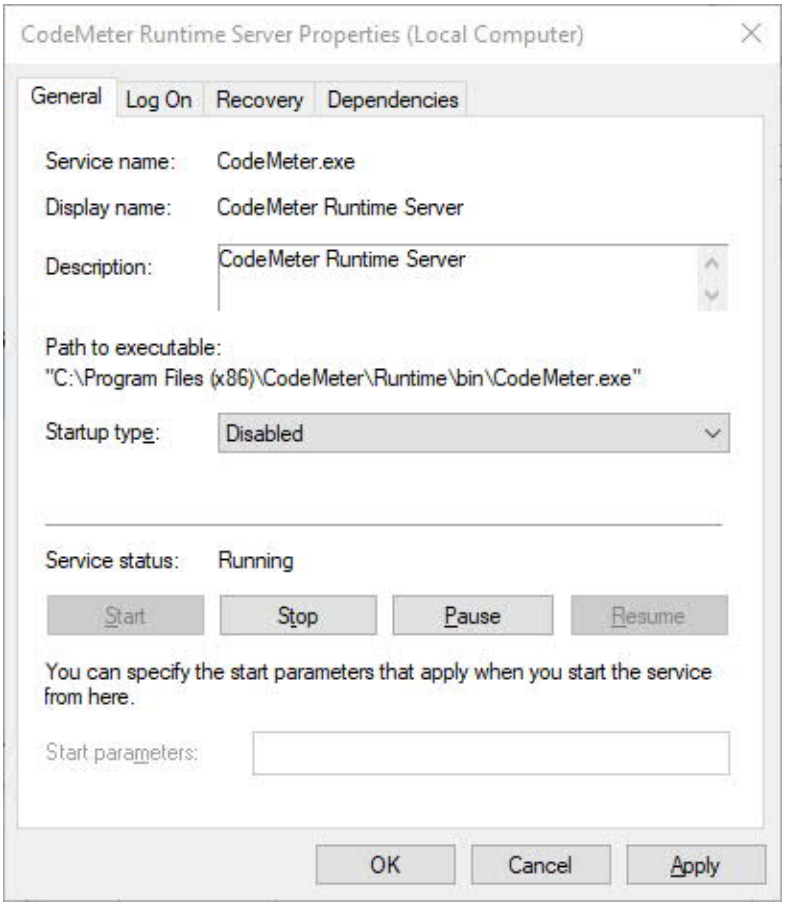
1) In windows search, type “Services”. Following application should be visible.

2) Select CodeMeter Runtime Server. In case the service is not in the list, make sure that the Services application is started in Local Administrator mode.



3) Select Stop to stop the CodeMeter Runtime Server.

4) Double-click the CodeMeter Runtime Server.



5) In Startup type, select Disabled.

6) Apply changes to the dialog by selecting Apply or OK.