DOCUMENT ID: 2NGA001822
REVISION: A
DATE: 2023-10-30

CYBER SECURITY ADVISORY

ABB COM600 CODESYS Vulnerabilities

CVE IDs:
CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393

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.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

ABB has identified that the COM600 product firmware versions

4.x and 5.x

are affected.

Vulnerability IDs

CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could cause the product to stop, make the product inaccessible or insert and run arbitrary code in the product.

Recommended immediate actions

ABB recommends that customers would perform the mitigating actions at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the COM600 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 or insert and run arbitrary code allowing the attacker to cause unwanted behavior in the product.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

Vulnerability severity and details

A set of 16 high-severity security flaws have been disclosed in the CODESYS V3 software development kit (SDK) that could result in remote code execution and denial-of-service under specific conditions, posing risks to operational technology (OT) environments.

CVSS number	CVSS score	Vulnerability	Exploit
CVE-2022-47378	6.5	Improper Validation of Consistency within Input	Denial-of-service
CVE-2022-47379	8.8	Out-of-bounds Write	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47380	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47381	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47382	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47383	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47384	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47385	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47386	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47387	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47388	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47389	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution
CVE-2022-47390	8.8	Stack-based Buffer Overflow	Denial-of-service, memory overwriting, remote code execution

[1] 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-2022-47391	7.5	Improper Validation of Consistency within Input	Denial-of-service
CVE-2022-47392	6.5	Improper Validation of Consistency within Input	Denial-of-service
CVE-2022-47393	6.5	Untrusted Pointer Dereference	Denial-of-service

CVE-2022-47378
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpFiletransfer component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47378

CVE-2022-47379
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to memory, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47379

CVE-2022-47380
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or re-mote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47380

CVE-2022-47381
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47381

CVE-2022-47382
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47382

CVE-2022-47383
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47383

CVE-2022-47384
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47384

CVE-2022-47385
After successful authentication, specific crafted communication requests can cause the CmpAppForce component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47385

CVE-2022-47386
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47386

CVE-2022-47387
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47387

CVE-2022-47388
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47388

CVE-2022-47389
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47389

CVE-2022-47390
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47390

CVE-2022-47391
CODESYS products such as the CODESYS Control runtime systems contain communication servers for the CODESYS protocol to enable communication with clients like the CODESYS Development System. Specific crafted communication requests with inconsistent content can cause the CmpDevice component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47391

CVE-2022-47392
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpApp/CmpAppBP/CmpAppForce components to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-47392

CVE-2022-47393
After successful authentication, specific crafted communication requests can cause the CmpFiletransfer component to dereference addresses provided by the request for internal read access, which can lead to a denial-of-service situation.

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-47393

Mitigating factors

The vulnerability can be mitigated by blocking the external access to the CODESYS components running on COM600 by using the Windows firewall. By default, two CODESYS components, Gateway Service and CodeMeter, are accessible through the firewall. The following instructions will show how to disable the external access to these two components and how to re-enable them if needed, for example when a new CODESYS or SAB600 configuration needs to be downloaded to COM600.

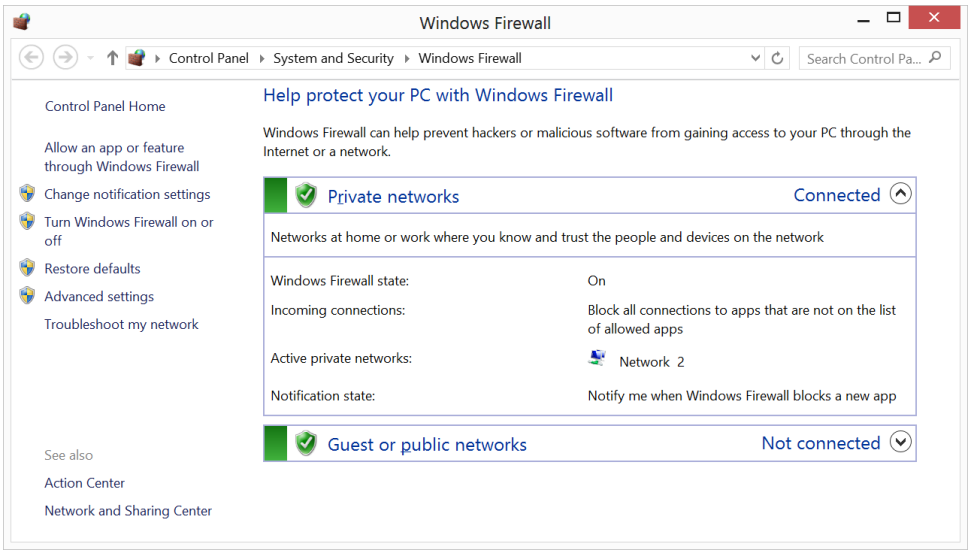
The user can either modify the Firewall settings manually using the Windows Firewall application, or automatically using provided script files. Both procedures are described below.

Note: When using the manual method, the CodeMeter service will automatically re-enable the “CodeMeter Runtime Server” rules whenever it is started, so this procedure must be redone after every COM600 reboot. The automated method is not affected by reboot.

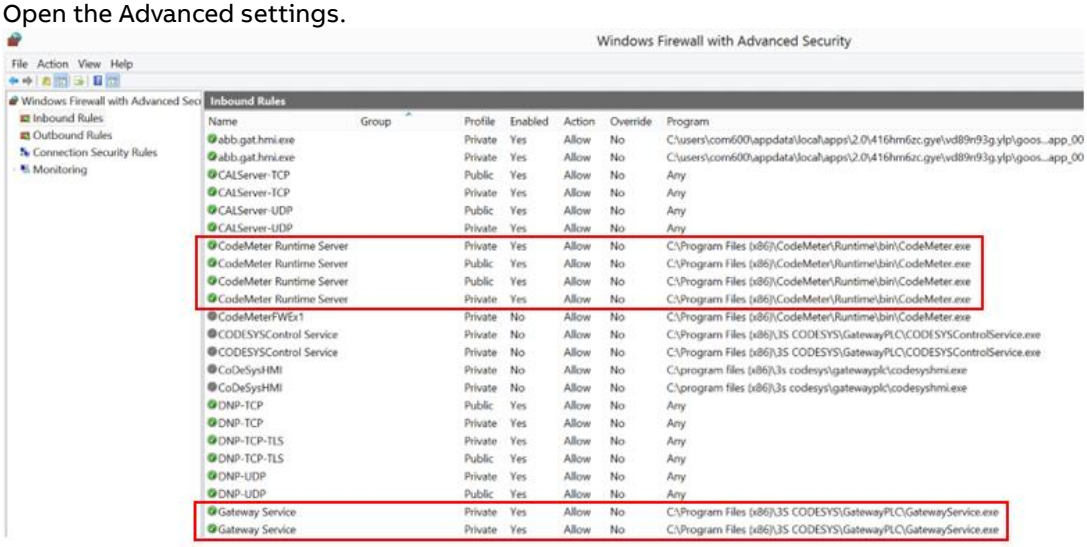
Modifying the Windows Firewall settings manually

Perform the following actions for manually disabling access to the CODESYS components.

1. Open the Windows Firewall from Windows settings.
2. Make sure that the Firewall is enabled for all networks (i.e., both Private and Public).

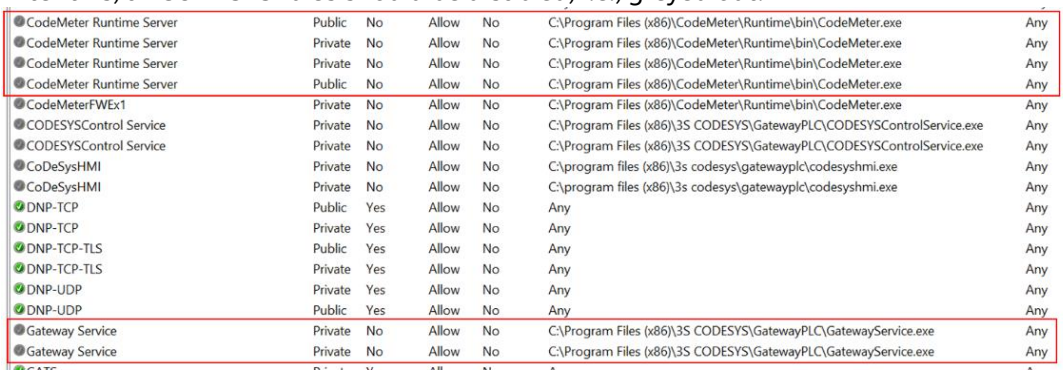


3. Open the Advanced settings.



   By default, the “CodeMeter Runtime Server” and “Gateway Service” CODESYS rules are enabled while “CoDeSysHMI”, “CODESYSControl Service” and “CodeMeterFWEx1” rules are disabled.

4. Right-click each of the six green CODESYS rules and select “Disable Rule” from the pop-up menu. After this, all CODESYS rules should be disabled, i.e., greyed out.



5. To re-enable the rules, if needed, open Advanced Settings again, and select “Enable Rule” for each of the rules disabled in step 4.

Refer to section “General security recommendations” for further advice on how to keep your system secure.

Modifying the Windows Firewall settings automatically

Perform the following steps for automating the firewall actions for blocking access to the CODESYS component. The automation is done by using Windows batch files (.bat) that are put to the root directory of the C-drive of COM600.

Three batch files will be created.

- A scheduled task for running the batch file that disables the CODESYS firewall rules shortly after the CodeMeter component has started
- Disable the Windows firewall rules for CODESYS components to protect them from external access
- Enable the Windows firewall rules for CODESYS components to allow access from CODESYS tools in the engineering computer.

1. In a Windows PC, copy the content of the Appendix A (without the “Appendix” header) to the Notepad. Do not add any line feeds to the “SCHTASKS” line, the command must be in one row. Save it with name `create_CodeSys_firewall_task.bat` to the PC.
2. In a Windows PC, copy the content of the Appendix B (without the “Appendix” header) to the Notepad. Save it with name `disable_CodeSys_firewall_rules.bat` to the PC.
3. In a Windows PC, copy the content of the Appendix C (without the “Appendix” header) to the Notepad. Save it with name `enable_CodeSys_firewall_rules.bat` to the PC.
4. Transfer the three files from the PC to the root directory of COM600 (C:\).
5. Run `disable_Codesys_firewall_rules.bat`
6. Run `create_codesys_firewall_task.bat`
7. The firewall configuration change can be tested by using CodeSys Logic Editor tool.
    a. Transferring the logic to COM600 should not be possible when the `disable_Codesys_firewall_rules.bat` has been run.
    b. Transferring the logic to COM600 should be possible when the `enable_CodeSys_firewall_rules.bat` has been run.
    c. After testing, make sure that the firewall rules are disabled by running again the `disable_Codesys_firewall_rules.bat` for disabling the access to the CODESYS component.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could send a specially crafted message to the system node, causing the node to stop, or become inaccessible or insert and run arbitrary code allowing the attacker to cause unwanted behavior in the product.

What causes the vulnerability?

There are multiple vulnerabilities in the CODESYS component. See the vulnerability table for details.

What is the CODESYS component?

The CODESYS component provides an internal logic processor for use via the OPC interfaces in COM600.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the node to stop or become inaccessible or insert and run arbitrary code.

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 they install malicious software on a system node or otherwise infect 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.

Can functional safety be affected by an exploit of this vulnerability?

Yes, by exploiting the vulnerability, the attacker may be able to e.g., send control commands.

What does the mitigation do?

The mitigation removes the vulnerability by modifying the firewall in such manner that the vulnerable component is not exposed to the network interfaces.

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

Yes, this vulnerability has been publicly disclosed.

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.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g., for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g., office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following documents:

Document ID: 1MRS758267, revision C, COM600 Cyber Security Deployment Guideline

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

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

Appendix A

```
@echo off

setlocal

REM Creates a Windows Scheduled task to disable the CodeSys firewall rules

REM since the CodeMeter service enables the firewall rules each time it starts.

REM This scheduled task runs the batch file that disables the CodeSys firewall

REM rules shortly after the CodeMeter has started.

set tasktorun=C:\disable_CodeSys_firewall_rules.bat

SCHTASKS /Create /TN "COM600\Disable CodeSys Firewall rules" /TR "%tasktorun%" /NP
/DELAY "0000:10" /SC ONEVENT /EC Application /MO
"*[System[Provider[@Name='CodeMeter Runtime Server'] and EventID=516]]"
```

Appendix B

```
@echo off
REM Disable the Windows firewall rules for CodeSys components to protect them
REM from external access.
REM Gateway Service was originally enabled for allowing the CodeSys
REM configuration tool access.
REM Must be enabled again if making changes to the configuration.
netsh advfirewall firewall set rule name="Gateway Service" new enable=no
REM CodeMeter Runtime Server will also be automatically enabled by the Codemeter
REM Service every time it starts.
REM To handle this, the script must be run each time after the service starts.
REM A Windows Scheduled Task is created for that purpose.
netsh advfirewall firewall set rule name="CodeMeter Runtime Server" new enable=no
REM The following rules are disabled by default, but disable them again
REM in case someone has turned them on.
netsh advfirewall firewall set rule name="CODESYSControl Service" new enable=no
netsh advfirewall firewall set rule name="CoDeSysHMI" new enable=no
netsh advfirewall firewall set rule name="CodeMeterFWEx1" new enable=no
```

Appendix C

```
@echo off
REM Enable the Windows firewall rules for CodeSys components to allow access by
REM CodeSys tools in engineering computer.
REM Gateway Service was originally enabled for allowing the CodeSys
REM configuration tool access.
REM Enabling it again for making changes to the configuration.
netsh advfirewall firewall set rule name="Gateway Service" new enable=yes
netsh advfirewall firewall set rule name="CodeMeter Runtime Server" new enable=yes
```

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	Oct-30-2023