

# Eaton Security Bulletin

## ETN-SB-2020-1011: Multiple security vulnerabilities in Wibu-Systems AG Codemeter Runtime

Date	Overall Risk	CVSS v3.0
10/5/2020 Updated 01/18/2021 Updated 03/04/2021	Critical	10.0

### Overview

[Cybersecurity and Infrastructure Security Agency \(CISA\)](#) has issued an [advisory](#) regarding multiple security vulnerabilities affecting Wibu-Systems AG Codemeter Runtime which is used in multiple products to protect against reverse engineering and to manage the licenses. Popular examples include 3S's Codesys Runtime that relies on CodeMeter Runtime for protecting the codes and managing the licenses. We are currently evaluating the impact of these vulnerabilities to our products and are developing mitigation plans to address them. Further information could be obtained from Wibu-Systems [Security advisory](#).

### Impacted Eaton Product(s) & Version(s)

The following Eaton products directly or indirectly utilize the 3S's Codesys Runtime and therefore are impacted by one or more of the reported vulnerabilities -

- XSOFT CODESYS Development System prior to V3.5.16

### Vulnerability Details

The impact of the reported vulnerabilities are varied and include classifications such as Buffer Access with Incorrect Length Value, Inadequate Encryption Strength, Origin Validation Error, Improper Input Validation, Improper Verification of Cryptographic Signature, Improper Resource Shutdown or Release.

For more details on the CVEs, please refer the below link for individual CVEs –

- [CVE-2020-14509](#)
- [CVE-2020-14517](#)
- [CVE-2020-14519](#)
- [CVE-2020-14513](#)
- [CVE-2020-14515](#)
- [CVE-2020-16233](#)

### Remediation & Mitigation

#### Remediation

# Eaton Security Bulletin

Eaton has patched the affected product and released a new version 3.5.16 for customers. The new version can be downloaded from here –

- [Download Center - Software \(eaton.eu\)](#) -> Software -> XSOFT-CODESYS -> 3.5.16

## Mitigation

Below are the options to minimize the risk of the issues in the affected systems –

### Option 1. – CodeMeter binded to localhost

- a) Open CodeMeter’s WebAdmin “Configuration” page.
- b) In the “Network” tab, disable “Run Network Server” AND configure the “Bind Address” to 127.0.0.1.
- c) Validate and restart the computer.

OR

- a) Open the Registry Editor and change the following keys under “Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion”:
  - i. IsNetworkServer=0; Disables server of the CodeMeter runtime
  - ii. BindAddress="127.0.0.1"; Set the BindAddress of the server of the CodeMeter runtime to localhost
  - iii. CmWebSocketApi=0; Disables WebSocket API

### HOW TO VALIDATE THE MORE SECURED SETUP

- i. Open a command prompt and enter the command “netstat -a -n”.
- ii. The customer should have only the localhost listening to the “Network Port” shown in CodeMeter’s WebAdmin (in the example below, port 22350 is used).

a. Should have	TCP	127.0.0.1:22350	0.0.0.0:0	LISTENING
b. Shouldn’t have	TCP	0.0.0.0:22350	0.0.0.0:0	LISTENING

### Option 2. – Upgrade CodeMeter

- a) Download and install CodeMeter version 7.10a or newer from: <https://www.wibu.com/support/user>.

### HOW TO VALIDATE THE MORE SECURED SETUP

- a) Validate that CodeMeter was installed successfully.

### Other best practices

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from business networks.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPNs are only as secure as the connected devices.
- Use an internal DNS server that performs DNS-over-HTTPS for lookups.
- Additional mitigation recommendations can be found in [ICS Advisory ICSA-20-203-01](#)

# Eaton Security Bulletin

## General Security Best Practices

- Restrict exposure to external networks for all control system devices and/or systems and ensure that they are not directly accessible from the open Internet.
- Deploy control system networks and remote devices behind barrier devices (e.g. firewalls, data diodes) and isolate them from business networks.
- Remote access to control system networks should be made available on a strict need-to-use basis. Remote access should use secure methods, such as Virtual Private Networks (VPNs), updated to the most current version available.
- Regularly update/patch software/applications to latest versions available, as applicable.
- Enable audit logs on all devices and applications.
- Disable/deactivate unused communication channels, TCP/UDP ports and services (e.g., SNMP, FTP, BootP, DHCP, etc.) on networked devices.
- Create security zones for devices with common security requirements using barrier devices (e.g. firewalls, data diodes).
- Change default passwords following initial startup. Use complex secure passwords or passphrases.
- Perform regular security assessments and risk analysis of networked control systems.

**For more details on cybersecurity best practices and leverage Eaton’s Cybersecurity as a Service, please consult the following –**

- Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology network. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security. More information about these services are available at [www.eaton.com/cybersecurityservices](http://www.eaton.com/cybersecurityservices). If you need immediate support, please call +1-800-498-2678 to connect with a representative.
- Cybersecurity Considerations for Electrical Distribution Systems ([WP152002EN](#))
- Cybersecurity Best Practices Checklist Reminder ([WP910003EN](#))

## Additional Support and Information

For additional information, including a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity web site [www.eaton.com/cybersecurity](http://www.eaton.com/cybersecurity), or contact us at [CybersecurityCOE@eaton.com](mailto:CybersecurityCOE@eaton.com).

### Legal Disclaimer:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO

## Eaton Security Bulletin

THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS AFFILIATES, OFFICERS, DIRECTORS, AND/OR EMPLOYEES, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF EATON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. EATON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

### **About Eaton:**

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, hydraulic and mechanical power more efficiently, safely and sustainably. Eaton is dedicated to improving the quality of life and the environment through the use of power management technologies and services. Eaton has approximately 100,000 employees and sells products to customers in more than 175 countries.

# Eaton Security Bulletin

## Revision Control:

Date	Version	Notes
10/5/2020	v1.0	Initial bulletin on the vulnerabilities.
01/18/2021	V1.1	Updated Mitigation steps
03/04/2021	V1.2	Updated Remediation for affected products

## Office:

Eaton, 1000 Eaton Boulevard  
Cleveland, OH 44122, United States  
Eaton.com