Eaton Security Bulletin

ETN-SB-2022-1004: CODESYS SECURITY ADVISORY

Date	Overall Risk	CVSS v3.0
05/22/2023	High	Multiple Vulnerabilities

1. Overview

CODESYS GmbH has issued multiple security advisories regarding vulnerabilities affecting various CODESYS software components. We are currently evaluating the impact of these vulnerabilities to our products and are developing mitigation plans to address them. Further information can be found on the CODESYS GmbH website.

2. Impacted Eaton Product(s) & Version(s)

From our preliminary assessments, the following Eaton products directly or indirectly utilize the affected CODESYS components and are therefore impacted by one or more of the reported vulnerabilities –

A. Form 7 recloser control, firmware v1.2.0 and earlier.
B. Proview NXG v2.3.0 and earlier *if* used in combination with CODESYS v3.5.17.10 and earlier to communicate with the Form 7 recloser control.
C. XSOFT-CODESYS V3 prior to v3.5.17 Bugfix 1
D. XV103 (CEAG) *if* used in combination with XSOFT-CODESYS version prior to v3.5.17 Bugfix 1
E. XC104/204 *if* used in combination with XSOFT-CODESYS version prior to v3.5.17 Bugfix 1
F. XC303 *if* used in combination with XSOFT-CODESYS version prior to v3.5.17 Bugfix 1

Note : The Proview NXG v2.3.0 and earlier alone is not impacted by the reported vulnerabilities. The impact is when used together with CODESYS.

3. Vulnerability Details

The impact of the reported vulnerabilities varies and if successfully exploited could allow an attacker to download and execute malicious code, cause a denial of service, or cause a device to restart unexpectedly. For more details on the reported vulnerabilities and associated CVEs, please refer to the following links:

- CODESYS Advisory 2021-02
  - CVE-2021-29240
- CODESYS Advisory 2021-03
  - CVE-2021-29239
- CODESYS Advisory 2021-04
  - CVE-2021-29241
- CODESYS Advisory 2021-12

    - CVE-2021-29241
- CODESYS Advisory 2021-13
    - CVE-2021-21863
    - CVE-2021-21864
    - CVE-2021-21865
    - CVE-2021-21866
    - CVE-2021-21867
    - CVE-2021-21868
    - CVE-2021-21869
- CODESYS Advisory 2022-02
    - CVE-2022-22515
- CODESYS Advisory 2022-04
    - CVE-2022-22517
- CODESYS Advisory 2022-05
    - CVE-2022-22518
- CODESYS Advisory 2022-06
    - CVE-2022-22513
    - CVE-2022-22514

4. Remediation

Eaton strongly recommends the implementation of the below remediation steps by updating the products to the latest firmware/software version.

- **Form 7 & ProView NXG products**

A. CODESYS advisories 2021-04 and 2021-12 were addressed in the latest version of firmware (v1.2.0) released for the Form 7 recloser control. Users with Form 7 controls running firmware versions earlier than v1.2.0 are advised to upgrade to v1.2.0, which includes an upgrade to CODESYS runtime version 3.5.17.10.

B. CODESYS advisories 2021-02, 2021-03, and 2021-13 were addressed with CODESYS software version 3.5.17.10 used with ProView NXG 3.4.0 and later. Users with Form 7 controls running CODESYS software version 3.5.15.10 with ProView NXG 3.3.0 or earlier are advised to upgrade to ProView NXG 3.4.0 and CODESYS software version 3.5.17.10. The Form 7 recloser control utilizes the CODESYS Control Runtime System Toolkit to manage, transfer, and execute logical application code developed by both Eaton and end users. Based on the components used in the Form 7 control, CODESYS advisories 2022-02, 2022-04, 2022-05, and 2022-06 apply to the latest firmware version of the Form 7 control running CODESYS runtime version 3.5.17.10.

Users are advised to download the latest CODESYS runtime version which includes the fixes for the above-mentioned vulnerabilities here.

- **XSOFT-CODESYS & XC/XV Products**

  The CODESYS advisories are addressed in the latest version of XSOFT-CODESYS 3.5.17 Bugfix 1.

Users are advised to download the latest XSOFT-CODESYS version which includes the fixes for the above-mentioned vulnerabilities here.

5. General Security Best Practices

5.1. Eaton recommends that customers follow cybersecurity best practices to further protect their devices and implement the following key procedures.

- 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.

5.2. For more Information on cybersecurity best practices and to 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 is available at 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

Additional 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, or contact us at CybersecurityCOE@eaton.com.

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. YOU ARE SOLELY RESPONSIBLE FOR REVIEWING THE USER MANUAL FOR YOUR DEVICES AND GAINING KNOWLEDGE OF CYBERSECURITY BEST PRACTICES. YOU SHOULD TAKE NECESSARY STEPS TO ENSURE THAT YOUR DEVICES ARE PROTECTED. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO 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, 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 85,000 employees and sells products to customers in more than 175 countries.

Revision Control:

Date	Version	Notes
04/25/2022	1.0	Initial Public advisory
11/30/2022	1.1	Updated remediation information related to the release of Form 7 firmware version 1.3.0.
05/22/2023	1.2	Updated advisory with updated list of impacted products and their remediation.

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com