Coordinated Disclosure Policy CODESYS GmbH

1 Introduction

Product security is of utmost importance to CODESYS GmbH. We are therefore highly committed to resolving vulnerabilities and to supporting the security and safety of industrial control systems, machines, plants or other devices operated with CODESYS software products.

CODESYS GmbH strongly recommends coordinated vulnerability disclosure. Only then do we have the opportunity to fix a flaw before it is publicly disclosed. Our aim is to provide our customers with high-quality security updates and to prevent them from being exposed to malicious attacks while the update is being developed.

This document describes how to report potential security vulnerabilities affecting the CODESYS software products to CODESYS GmbH and how customers are informed by CODESYS GmbH about verified vulnerabilities, resolutions and mitigations.

2 Reporting of vulnerabilities

CODESYS GmbH strongly encourages the reporting of possible vulnerabilities or other security issues. We ask anyone who discovers a vulnerability affecting the CODESYS software products to report it directly to us. As mentioned above, an immediate public disclosure may encourage a malicious attack and cause serious security risks for control systems, machines, plants or other devices operated with CODESYS software products. All vulnerability reports are handled with utmost care and the interests of the reporting party are respected and observed.

Discovered vulnerabilities should be reported using our web form under www.codesys.com/security or per email to the CODESYS Security Team at security@codesys.com.
Reporting parties who provide their email address will receive a prompt acknowledgement of receipt and will be contacted for follow-up.

When reporting a vulnerability or other security issues please include the following information:

- Name and version of the affected product
- Description of vulnerability
- Publicity of vulnerability

3 Internal vulnerability handling

All security vulnerabilities reported to CODESYS GmbH are thoroughly investigated, assessed and prioritized. Goal is to identify all possibly affected products, determine the root cause of the vulnerability, and develop a resolution or remediation. CODESYS GmbH may possibly request more information from the reporter in this process.

CODESYS GmbH may inform official CERTs and interested OEMs and maintain active communication with these and the reporting party to inform about remediation and software updates. If available, pre-releases of software fixes can be provided to the reporter for verification.

4 Disclosure

Once a mitigation or resolution (usually software update) is available, CODESYS GmbH will release an advisory. This advisory is published on the CODESYS website under www.codesys.com/security.

In some cases, disclosure may be limited to a specific group of customers. These customers are contacted directly and the advisory in question is published in the password protected customers area on the CODESYS website only. As each security vulnerability case is different, we may take alternative actions if necessary.

A CODESYS advisory usually contains the following:

- Description of the vulnerability and its severity (based on CVSS score)
- Identification of products and versions affected
- Information on mitigating factors and workarounds
- Timeline and availability of software security updates
- With the reporting party's consent, credit is provided for reporting and collaboration

5 Contact information

Website: www.codesys.com/security

Email: security@codesys.com

6 Disclaimer

CODESYS GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by CODESYS GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of CODESYS GmbH.
Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact support@codesys.com.

Change History

Version	Description	Date
1.0	First version	25.04.2017
1.1	Adjustments change of name	29.06.2021