OSCAT Basic library

CODESYS Security Advisory 2024-04

Published: 2024-09-12

1 Overview

The OSCAT Basic library is one of several libraries developed and provided by OSCAT. OSCAT (http://oscat.de/) stands for "Open Source Community for Automation Technology".

The OSCAT Basic library offers function blocks for various tasks, e.g. for buffer management, list processing, control technology, mathematics, string processing, time and date conversion. By adding the OSCAT Basic library into IEC 61131-3-compliant programming tools, PLC programmers can use all the functions provided by the library in their control programs.

Within the library, the MONTH_TO_STRING function is affected by an out-of-bounds read vulnerability. Exploitation of the vulnerability may lead to limited access to internal data or possibly to a crash of the PLC.

2 Affected Products

The OSCAT Basic library is affected in all versions prior to 3.3.5. It is developed and provided by OSCAT, the "Open Source Community for Automation Technology".

Note: In the OSCAT version history, version 3.3.5 is listed as 335 (without dots). In the CODESYS Store, the same version is named 3.3.5.0.

3 Vulnerability Identifiers, Type and Severity

VDE-2024-046 [1]

CODESYS JIRA: STORE-4586

CVE-2024-6876 [7]

CWE-125: Out-of-bounds Read [8]

CVSS v3.1 Base Score 5.1 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L [9]

4 Impact

The OSCAT Basic library, which is developed and provided by OSCAT, the "Open Source Community for Automation Technology", as an extension to the IEC 61131-3-based programming tools, offers functions for a wide range of programming tasks. As part of the date and time processing functions, the library offers a function called MONTH_TO_STRING for converting months into various selectable string representations.

The MONTH_TO_STRING function of the OSCAT Basic library does not completely check the valid ranges of the passed values. This poses a vulnerability for the programmed PLC if values are passed to the MONTH_TO_STRING function that are fed into the PLC program from outside. An example could be a visualization in which integer values can be entered, which are then passed directly from the PLC program without further range checking as parameters to the MONTH_TO_STRING function. By entering values outside the valid range, an attacker can perform out-of-bounds read accesses to read limited internal data from the PLC or possibly cause it to crash.

5 Remediation

Update the OSCAT Basic library to version 3.3.5.

The OSCAT Basic library 3.3.5 can be downloaded from the CODESYS Store [4] as version 3.3.5.0 or alternatively directly from the OSCAT website http://oscat.de/.

To make the fix effective for existing CODESYS projects, you also must adjust the version of the OSCAT Basic library to be used in the Library Manager of the CODESYS project to version 3.3.5.0. Then you must update the CODESYS application on the PLC by download or online change and rebuild/download the boot application.

Template: templ_tecdoc_en_V3.0.docx

6 Mitigation

CODESYS GmbH recommends an update of the OSCAT Basic library to address the security vulnerability. Without an update, the vulnerability can be prevented by validating all values in the PLC program before they are passed to the affected function. In particular, negative values must be blocked as function parameters of MONTH_TO_STRING.

Regardless of whether the OSCAT Basic library in the programming system was updated or the security vulnerability in the PLC program was mitigated, a download or online change must be performed to update the application on the PLC. And don't forget to rebuild/download the boot project.

7 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside

• Use firewalls to protect and separate the control system network from other networks

• Activate and apply user management and password features

• Limit the access to both development and control system by physical means, operating system features, etc.

• Use encrypted communication links

• Use VPN (Virtual Private Networks) tunnels if remote access is required

• Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [2].

8 Acknowledgments

This issue was reported by Corban Villa, Hithem Lamri, Constantine Doumanidis, Michail Maniatakos of Modern Microprocessors Architecture (MoMA) Lab at NYU Abu Dhabi.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

9 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support team [6].

10 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 sales@codesys.com.

11 Bibliography

[1] CERT@VDE: https://cert.vde.com
[2] CODESYS GmbH: CODESYS Security Whitepaper
[3] CODESYS GmbH: Coordinated Disclosure Policy
[4] CODESYS GmbH download area: https://www.codesys.com/download
[5] CODESYS GmbH security information page: https://www.codesys.com/security
[6] CODESYS GmbH support contact site: https://www.codesys.com/support
[7] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[8] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[9] CVSS Calculator: https://www.first.org/cvss/calculator/3.1

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=18601&token=27389a52e058d95ff70b17a2370fedf07e073034&download=

Change History

Version	Description	Date
1.0	Initial version	2024-08-29
2.0	Software update available	2024-09-10
3.0	VDE reference added	2024-09-12