SSA-944952: Authentication Bypass Vulnerability in Opcenter Quality

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 9.6

SUMMARY

Siemens has released updates for Opcenter Quality to fix an authentication bypass vulnerability. This could allow unauthenticated access to the application or cause denial of service condition for existing users. The issue is based on rich client modules using IbsGailWrapper-interface. After issuing the record the authentication bypass vulnerability could take place on all modules.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Opcenter Quality V13.1: All versions < V13.1.20220624	Update to V13.1.20220624 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Opcenter Quality V13.2: All versions < V13.2.20220624	Update to V13.2.20220624 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Solutions with configuration as Encrypted=2 in ibs.config are potentially impacted by this vulnerability. If problems exists and an immediate replace of IbsGailWrapper.dll is NOT possible, please contact your support-team to change the secure mode of your installation
- For all other cases it is recommended to replace the IbsGailWrapper.dll for short-term

Product specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Opcenter Quality is a quality management system (QMS) that enables organizations to safeguard compliance, optimize quality, reduce defect and rework costs and achieve operational excellence by increasing process stability. The integrated process capabilities (control charts, statistics, quality gates) can detect production errors to avoid further processing and shipment of nonconforming material.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-33736

The affected applications do not properly validate login information during authentication. This could lead to denial of service condition for existing users or allow unauthenticated remote attackers to successfully login without credentials.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-303: Incorrect Implementation of Authentication Algorithm

ADDITIONAL INFORMATION

For more information refer to the related article in the support center:

- Opcenter Quality: https://support.sw.siemens.com/en-US/knowledge-base/PL8657076

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-07-12): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.