# SSA-788287: Disclosure of Private Data

Publication Date: 2021-04-13
Last Update: 2021-04-13
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

## SUMMARY

Due to SmartClient Installation technology (ClickOnce) a customer/integrator needs to create a customer specific Smartclient installer. The mentioned products delivered a trusted but yet expired codesigning certificate.

An attacker could have exploited the vulnerability by spoofing the code-signing certificate and signing a malicious executable resulting in having a trusted digital signature from a trusted provider.

The certificate was revoked immediately.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Opcenter Quality:<br>All versions < V12.2 | See recommendations from section Workarounds and Mitigations |
| QMS Automotive:<br>All versions < V12.30 | See 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:

- Explicitly distrust the certificate with the fingerprint FA:53:A4:74:FC:1E:16:6F:E6:6A:D2:5A:C1:E6:8B:B1:91:CB:38:E9:85:7E:07:79:C1:A5:C3:59:1A:5A:04:96
- The certificate expired on 7th March 2021 and was not renewed.
- Make sure to use correct Certificate validation (CRL / OSCP) when validating certificates.

## 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 (formerly known as "CAQ=QSYS") 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-2021-27389

A private sign key is shipped with the product without adequate protection.

| | |
|---|---|
| CVSS v3.1 Base Score | 10.0 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

## ADDITIONAL INFORMATION

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 (2021-04-13): 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.