SSA-408105: Buffer Overflow Vulnerabilities in OpenSSL 3.0 Affecting Siemens Products

Publication Date: 2022-12-13
Last Update: 2023-07-11
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

The openSSL component, versions 3.0.0 through 3.0.6, contains two buffer overflow vulnerabilities (CVE-2022-3602, CVE-2022-3786) in the X.509 certificate verification [0]. They could allow an attacker to create a denial of service condition or execute arbitrary code on a vulnerable TLS server (if the server requests client certificate authentication), or on a vulnerable TLS client.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

[0] https://www.openssl.org/news/secadv/20221101.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Calibre ICE: All versions >= V2022.4 < V2023.1	Update to V2023.1 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Mcenter: All versions >= V5.2.1 < V5.3.0	Update to V5.3.0 or later version https://download.industrysoftware.automation.siemens.com/ As a mitigation for vulnerable versions: Ensure that only trusted (CA) certificates are contained in the Machine Agent's truststore See further recommendations from section Workarounds and Mitigations
SCALANCE X-200RNA switch family: All versions >= V3.2.7	Currently no fix is available See recommendations from section Workarounds and Mitigations
SICAM GridPass (6MD7711-2AA00-1EA0): All versions >= V1.80 < V2.20	Update to V2.20 or later version https://support.industry.siemens.com/cs/ww/en/view/109763384/ As a mitigation for vulnerable versions: In the truststore, do not add CA certificates that contain a nameConstraint-extension (https://www.rfc-editor.org/rfc/rfc5280#section-4.2.1.10) with punycode-encoded internationalized domain names See further recommendations from section Workarounds and Mitigations

SIMATIC RTLS Locating Manager: All versions >= V2.13 < V2.13.0.3	Update to V2.13.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109821005/ 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:

- Siemens products that contain a vulnerable TLS server and have certificate-based client authentication enabled: do not configure trust for CA certificates, that contain a nameConstraint-extension (https://www.rfc-editor.org/rfc/rfc5280#section-4.2.1.10) with punycode-encoded internationalized domain names
- Siemens products that contain a vulnerable TLS client: in cases where this option is configurable: ensure that TLS server certificate verification is turned on and do not configure trust for CA certificates, that contain a nameConstraint-extension (https://www.rfc-editor.org/rfc/rfc5280#section-4.2.1.10) with punycode-encoded internationalized domain names

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

Calibre ICE (IC Cloud Enablement) enables Calibre products and other products of the IC segment to make use of cloud services.

Mcenter (formerly called SINUMERIK Integrate) is an open platform to manage all types of machines - regardless of their controller type and age - covering the complete shopfloor and providing detailed insights about tools, NC programs and machine utilization.

SIMATIC RTLS Locating Manager is used for the configuration, operation, and maintenance of a SIMATIC RTLS installation, which is real-time wireless locating system for flexible and cost-effective locating solutions.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SICAM GridPass is an easy to manage PKI (public key infrastructure) product which creates and manages X.509 standardized certificates.

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-2022-3602

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-3786

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the '.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

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 (2022-12-13):	Publication Date
V1.1 (2023-04-11):	Added fix for Calibre ICE and SICAM GridPass
V1.2 (2023-07-11):	Added fix for Mcenter (SINUMERIK Integrate) and for SIMATIC RTLS Locating Manager

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.