SSA-953464: Multiple Vulnerabilites in Siemens Brownfield Connectivity - Client before V2.15

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Siemens has released a new version for Brownfield Connectivity - Client that contains fixes for multiple vulnerabilities in the underlying OpenSSL library. Successful exploitation of these vulnerabilities could lead to Denial of Service (DoS).

Siemens has released an update for Brownfield Connectivity - Client and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Brownfield Connectivity - Client: All versions < V2.15	Update to V2.15 or later version Contact customer support to obtain the update

WORKAROUNDS AND MITIGATIONS

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

Brownfield Connectivity – Client is a Software, which is installed on SINUMERIK and collects PLC & NC data and send them to the Brownfield Connectivity – Gateway.

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-2022-1292

The c_rehash script does not properly sanitise shell metacharacters to prevent command injection.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2022-1343

Under certain circumstances, the command line OCSP verify function reports successful verification when the varification in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2022-1434

When using the RC4-MD5 ciphersuite, which is disabled by default, an attacker is able to modify data in transit due to an incorrect use of the AAD data as the MAC key in OpenSSL 3.0. An attacker is not able to decrypt any communication.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2022-1473

The used OpenSSL version improperly reuses memory when decoding certificates or keys. This can lead to a process termination and Denial of Service for long lived processes.

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-404: Improper Resource Shutdown or Release

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 (2023-02-14): Publication Date

TERMS OF USE