SSA-744259: Golang Vulnerabilities in Brownfield Connectivity - Gateway before V1.10.1

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

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

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Brownfield Connectivity - Gateway: All versions < V1.10	Update to V1.11 or later version Contact customer support to obtain the update https://support.industry.siemens.com/cs/de/de/view/109801700
Brownfield Connectivity - Gateway: V1.10.1 only affected by CVE-2022-24675, CVE-2022-27536, CVE-2022-28327	Update to V1.11 or later version Contact customer support to obtain the update https://support.industry.siemens.com/cs/de/de/view/109801700

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 – Gateway collects data from the configured clients and forwards the data to other connected systems.

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-2021-41771

ImportedSymbols in debug/macho (for Open or OpenFat) in Go before 1.16.10 and 1.17.x before 1.17.3 Accesses a Memory Location After the End of a Buffer, aka an out-of-bounds slice situation.

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-41772

Go before 1.16.10 and 1.17.x before 1.17.3 allows an archive/zip Reader.Open panic via a crafted ZIP archive containing an invalid name or an empty filename field.

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-20: Improper Input Validation

Vulnerability CVE-2021-44716

net/http in Go before 1.16.12 and 1.17.x before 1.17.5 allows uncontrolled memory consumption in the header canonicalization cache via HTTP/2 requests.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2021-44717

Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network connection as a consequence of erroneous closing of file descriptor 0 after file-descriptor exhaustion.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2022-24675

encoding/pem in Go before 1.17.9 and 1.18.x before 1.18.1 has a Decode stack overflow via a large amount of PEM data.

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-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-24921

regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion via a deeply nested expression.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-27536

Certificate.Verify in crypto/x509 in Go 1.18.x before 1.18.1 can be caused to panic on macOS when presented with certain malformed certificates. This allows a remote TLS server to cause a TLS client to panic.

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-295: Improper Certificate Validation

Vulnerability CVE-2022-28327

The generic P-256 feature in crypto/elliptic in Go before 1.17.9 and 1.18.x before 1.18.1 allows a panic via long scalar input.

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-20: Improper Input Validation

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

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.