SSA-555292: Security Vulnerabilities Fixed in SIMATIC Cloud Connect 7 V2.1

Publication Date: 2023-05-09
Last Update: 2023-05-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.2

SUMMARY

SIMATIC Cloud Connect 7 contains multiple vulnerabilities that could allow an attacker to impact its confidentiality, integrity and availability.

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
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions >= V2.0 < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109818318/
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions < V2.1 only affected by CVE-2023-29103, CVE-2023-29105	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109818318/
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions >= V2.0 < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109818318/
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions < V2.1 only affected by CVE-2023-29103, CVE-2023-29105	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109818318/

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

SIMATIC Cloud Connect 7 is an IoT Gateway to connect programmable logic controllers to cloud services and enables the connection of field devices with OPC UA server Interface as OPC UA clients.

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-2023-28832

The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-29103

The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-259: Use of Hard-coded Password

Vulnerability CVE-2023-29104

The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to.

CVSS v3.1 Base Score	6.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2023-29105

The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS).

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:N/A:H/E:P/RL:O/RC:C
CWE	CWE-544: Missing Standardized Error Handling Mechanism

Vulnerability CVE-2023-29106

The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2023-29107

The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-552: Files or Directories Accessible to External Parties

Vulnerability CVE-2023-29128

The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`.

CVSS v3.1 Base Score	3.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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 (2023-05-09):	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.