SSA-995338: Multiple Vulnerabilities in COMOS Web

Publication Date:	2022-01-11
Last Update:	2022-04-12
Current Version:	V1.2
CVSS v3.1 Base Score:	8.8

SUMMARY

Multiple vulnerabilities were identified in the web components of COMOS that could allow an attacker to conduct code injections, store data in undesired locations, execute arbitrary SQL statements, and run cross-site request forgery attacks.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
COMOS V10.2: All versions only if web components are used	Currently no fix is planned See recommendations from section Workarounds and Mitigations
COMOS V10.3: All versions < V10.3.3.3 only if web components are used	Update to V10.3.3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109808862/ See further recommendations from section Workarounds and Mitigations
COMOS V10.3: All versions >= V10.3.3.3 only if web components are used only affected by CVE-2021-37196	Currently no fix is planned See recommendations from section Workarounds and Mitigations
COMOS V10.4: All versions < V10.4.1 only if web components are used	Update to V10.4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109805632/ See further 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:

- For **COMOS V10.4.1** / **V10.3.3.3** and **CVE-2021-37194**: Use the new whitelisting feature, to specify the filetypes that are allowed to be uploaded
- **CVE-2021-37196** can be mitigated in all versions by making the root directory of the web server read only

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

COMOS is a unified data platform for collaborative plant design, operation and management that supports collecting, processing, saving, and distributing of information throughout the entire plant lifecycle.

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-2021-37194

The COMOS Web component of COMOS allows to upload and store arbitrary files at the webserver. This could allow an attacker to store malicious files.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2021-37195

The COMOS Web component of COMOS accepts arbitrary code as attachment to tasks. This could allow an attacker to inject malicious code that is executed when loading the attachment.

CVSS v3.1 Base Score	7.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2021-37196

The COMOS Web component of COMOS unpacks specially crafted archive files to relative paths. This vulnerability could allow an attacker to store files in any folder accessible by the COMOS Web webservice.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-23: Relative Path Traversal

Vulnerability CVE-2021-37197

The COMOS Web component of COMOS is vulnerable to SQL injections. This could allow an attacker to execute arbitrary SQL statements.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2021-37198

The COMOS Web component of COMOS uses a flawed implementation of CSRF prevention. An attacker could exploit this vulnerability to perform cross-site request forgery attacks.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Sandro Poppi for reporting the vulnerabilities

ADDITIONAL INFORMATION

Updated general product information and user manuals are available on SIOS Portal. Please also consider the Security-relevant configuration for COMOS.

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 (2022-01-11):	Publication Date
V1.1 (2022-02-08):	Added CVE-2021-37194 and Updated Affected Products
V1.2 (2022-04-12):	Updated remediation for COMOS V10.3

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.