SSA-693110: Buffer Overflow Vulnerability in COMOS

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

COMOS is affected by memory corruption vulnerability in the cache validation service that could allow an attacker to execute arbitrary code or cause denial of service condition.

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
COMOS V10.2: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
COMOS V10.3.3.1: All versions < V10.3.3.1.45	Update to V10.3.3.1.45 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations
COMOS V10.3.3.2: All versions < V10.3.3.2.33	Update to V10.3.3.2.33 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations
COMOS V10.3.3.3: All versions < V10.3.3.3.9	Update to V10.3.3.3.9 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations
COMOS V10.3.3.4: All versions < V10.3.3.4.6	Update to V10.3.3.4.6 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations

COMOS V10.4.0.0: All versions < V10.4.0.0.31	Update to V10.4.0.0.31 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations
COMOS V10.4.1.0: All versions < V10.4.1.0.32	Update to V10.4.1.0.32 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) See recommendations from section Workarounds and Mitigations
COMOS V10.4.2.0: All versions < V10.4.2.0.25	Update to V10.4.2.0.25 or later version The patch is available on request from customer support. Alternatively, update to V10.4.3 or later version (available for download at https://support.industry.siemens.com/cs/ww/en/view/109815702/) 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:

- Enable Structured Exception Handling Overwrite Protection (SEHOP) in your Windows Operating System where COMOS is installed to protect against code execution. However, the application is still vulnerable to denial of service attacks

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-2023-24482

Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ADDITIONAL INFORMATION

This vulnerability has been discovered internally by Siemens.

Updated general product information and user manuals are available on SIOS Portal: https://support.industry.siemens.com/cs/ww/en/view/109739837.
Please also consider the Security-relevant configuration for COMOS: https://support.industry.siemens.com/cs/ww/en/view/109815213/.

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.