SSA-137900: Multiple Vulnerabilities in COMOS

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

COMOS is affected by multiple vulnerabilities that could allow an attacker to execute arbitrary code or cause denial of service condition, data infiltration or perform access control violations.

Siemens has released an update for COMOS and recommends to update to the latest version. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
COMOS: All versions < V10.4.4 affected by CVE-2020-25020, CVE-2020-35460, CVE-2022-23095, CVE-2022-28807, CVE-2022-28808, CVE-2022-28809, CVE-2023-0933, CVE-2023-1530, CVE-2023-2931, CVE-2023-2932, CVE-2023-22669, CVE-2023-22670, CVE-2023-43503, CVE-2023-43504	Update to V10.4.4 or later version For CVE-2023-43503, update to V10.4.4 or later version and update the COMOS database to version 25. (See “Data maintenance: Modifying the version” in the user manual. Warning: After the update, the database cannot be used by older COMOS versions) For CVE-2023-43504, delete ptmcast.exe from bin folder of COMOS installation directory. Installations from COMOS V10.4.4 or later version does not contain ptmcast.exe https://support.industry.siemens.com/cs/ww/en/view/109824522/ See further recommendations from section Workarounds and Mitigations
COMOS: All versions affected by CVE-2023-43505, CVE-2023-46601	Currently no fix is planned 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:

- Ensure all files imported into COMOS originate from a trusted source and transmitted are over secure channels
- CVE-2023-43505, CVE-2023-46601: Use an application server like Citrix which builds an additional layer of access control around COMOS. The file share with the documents folder and the database should be only accessible by the application server. You can find further recommendations in the COMOS manual “Securityrelevant configuration” in COMOS documentation (https://support.industry.siemens.com/cs/document/109823629/)

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-2020-25020

MPXJ through 8.1.3 allows XXE attacks. This affects the GanttProjectReader and PhoenixReader components.

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-611: Improper Restriction of XML External Entity Reference

Vulnerability CVE-2020-35460

common/InputStreamHelper.java in Packwood MPXJ before 8.3.5 allows directory traversal in the zip stream handler flow, leading to the writing of files to arbitrary locations.

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-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2022-23095

Open Design Alliance Drawings SDK before 2022.12.1 mishandles the loading of JPG files. Unchecked input data from a crafted JPG file leads to memory corruption. An attacker can leverage this vulnerability to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-28807

Open Design Alliance Drawings SDK (all versions prior to 2023.2) is vulnerable to an out-of-bounds read when rendering DWG files after they are opened in the recovery mode. This could allow an attacker to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-28808

Open Design Alliance Drawings SDK (all versions prior to 2023.3) is vulnerable to an out-of-bounds read when reading DWG files in a recovery mode. This could allow an attacker to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-28809

Open Design Alliance Drawings SDK (all versions prior to 2023.3) is vulnerable to an out-of-bounds read when reading a DWG file with invalid vertex number in a recovery mode. This could allow an attacker to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-0933

Integer overflow in PDFium library used in COMOS allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2023-1530

Use after free in PDFium library used in COMOS allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2023-2931

Use after free in PDFium library used in COMOS allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2023-2932

Use after free in PDFium library used in COMOS allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2023-22669

Open Design Alliance Drawings SDK used in affected application is vulnerable to heap-based buffer overflow while parsing specially crafted DWG files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19104)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-22670

Open Design Alliance Drawings SDK used in affected application is vulnerable to heap-based buffer overflow while parsing specially crafted DXF files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19382)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-43503

Caching system in the affected application leaks sensitive information such as user and project information in cleartext via UDP.

CVSS v3.1 Base Score	3.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2023-43504

Ptmcast executable used for testing cache validation service in affected application 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	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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’)

Vulnerability CVE-2023-43505

The affected application lacks proper access controls in SMB shares. This could allow an attacker to access files that the user should not have access to.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2023-46601

The affected application lacks proper access controls in making the SQLServer connection. This could allow an attacker to query the database directly to access information that the user should not have access to.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ADDITIONAL INFORMATION

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/document/109823629/.

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK refer to the ODA Security Advisories at https://www.opendesign.com/security-advisories.

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 (2023-11-14): 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.