SSA-155599: File Parsing Vulnerabilities in COMOS

Publication Date:	2022-03-08
Last Update:	2022-03-08
Current Version:	V1.0
CVSS v3.1 Base Score:	7.8

SUMMARY

COMOS uses Drawings SDK from Open Design Alliance that is affected by multiple vulnerabilities that could be triggered when the application reads files in DGN, DXF or DWG file formats. If a user is tricked to open a malicious file with the affected application, an attacker could leverage the vulnerability to leak information or potentially perform remote code execution in the context of the current process.

Siemens has released an update for the COMOS and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
COMOS: All versions < V10.4.1	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:

- Avoid to open untrusted files from unknown sources in COMOS

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-2021-25173

Open Design Alliance Drawings SDK before 2021.12 contains a memory allocation with excessive size vulnerability while parsing specially crafted DGN files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-12019)

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-789: Memory Allocation with Excessive Size Value

Vulnerability CVE-2021-25174

Open Design Alliance Drawings SDK before 2021.12 contains a memory allocation with excessive size vulnerability while parsing specially crafted DGN files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-12026)

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-789: Memory Allocation with Excessive Size Value

Vulnerability CVE-2021-25175

Open Design Alliance Drawings SDK before 2021.11 contains a type conversion vulnerability while parsing specially crafted DXF and DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-11912, ZDI-CAN-11993, ZDI-CAN-11988)

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-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-25176

Open Design Alliance Drawings SDK before 2021.11 contains a NULL pointer dereference vulnerability while parsing DXF and DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-11913, ZDI-CAN-11989)

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-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-25177

Open Design Alliance Drawings SDK before 2021.11 contains a type confusion issue while parsing specially crafted DXF and DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-11927)

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-843: Access of Resource Using Incompatible Type (‘Type Confusion’)

Vulnerability CVE-2021-25178

Open Design Alliance Drawings SDK before 2021.11 contains a stack-based buffer overflow vulnerability while parsing specially crafted DXF or DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-11901, ZDI-CAN-12165, ZDI-CAN-12166)

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2021-31784

Open Design Alliance Drawings SDK before 2021.6 contains an out-of-bounds write issue while parsing specially crafted DXF files. This could result in a write past the end of an allocated buffer and allow an attacker to execute code in the context of the current process. (ZDI-CAN-11915)

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-2021-32936

Open Design Alliance Drawings SDK before 2022.4 contains an out-of-bounds write issue while parsing specially crafted DXF files. This could result in a write past the end of an allocated buffer and allow an attacker to execute code in the context of the current process. (ZDI-CAN-13408)

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-2021-32938

Open Design Alliance Drawings SDK before 2022.4 are vulnerable to an out-of-bounds read while parsing specially crafted DWG files. This could allow an attacker to read sensitive information from memory locations and to cause a denial of service (crash). (ZDI-CAN-13378)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-32940

Open Design Alliance Drawings SDK before 2022.4 are vulnerable to an out-of-bounds read while parsing specially crafted DWG files. This could allow an attacker to read sensitive information from memory locations and to cause a denial of service. (ZDI-CAN-13412)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-32944

Open Design Alliance Drawings SDK before 2021.11 contains a use-after-free vulnerability while parsing specially crafted DGN files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-13468, ZDI-CAN-13413)

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-416: Use After Free

Vulnerability CVE-2021-32946

Open Design Alliance Drawings SDK before 2022.4 are vulnerable to improper check for unusual or exceptional conditions while parsing specially crafted DGN files. This could allow an attacker to cause a denial-of-service condition or execute code in the context of the current process. (ZDI-CAN-13411, ZDI-CAN-13409)

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-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2021-32948

Open Design Alliance Drawings SDK before 2022.4 contains an out-of-bounds write issue while parsing specially crafted DWG files. This could result in a write past the end of an allocated buffer and allow an attacker to execute code in the context of the current process. (ZDI-CAN-13410)

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-2021-32950

Open Design Alliance Drawings SDK before 2022.4 are vulnerable to an out-of-bounds read while parsing specially crafted DXF files. This could allow an attacker to read sensitive information from memory locations and to cause a denial of service. (ZDI-CAN-13415)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-32952

Open Design Alliance Drawings SDK before 2022.4 contains an out-of-bounds write issue while parsing specially crafted DGN files. This could result in a write past the end of an allocated buffer and allow an attacker to execute code in the context of the current process. (ZDI-CAN-13417)

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

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK refer to:

- ODA Security Advisories : 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 (2022-03-08):	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.