SSA-975766: Open Design Alliance Drawings SDK Vulnerability in Solid Edge

Publication Date: 2023-06-13
Last Update: 2023-11-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

Solid Edge is affected by a file parsing vulnerability in Drawings SDK from Open Design Alliance. If a user is tricked to open a malicious DWG file with the affected application, an attacker could leverage the vulnerability to crash the application or execute arbitrary code.

Siemens has released updates for the affected products and recommends to update to the latest versions.

Note:

- This advisory covers security vulnerabilities recently disclosed by Open Design Alliance [0]

[0] https://www.opendesign.com/security-advisories

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2023: All versions < V223.0 Update 5	Update to V223.0 Update 5 or later version https://support.sw.siemens.com/ 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 Solid Edge

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

Solid Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing and design management.

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-2023-26495

Open Design Alliance Drawings SDK (versions before 2024.1) contains a use-after-free vulnerability that could be triggered while parsing specially crafted DWG file. An attacker could leverage this in conjunction with other vulnerabilities to execute arbitrary code. (ZDI-CAN-19162, ZDI-CAN-19432)

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Open Design Alliance for coordination efforts

ADDITIONAL INFORMATION

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 (2023-06-13): Publication Date
V1.1 (2023-11-14): Updated description and CWE for CVE-2023-26495

TERMS OF USE