SSA-491245: Multiple File Parsing Vulnerabilities in Solid Edge

Publication Date: 2023-02-14
Last Update: 2023-03-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

Solid Edge is affected by multiple memory corruption vulnerabilities that could be triggered when the application reads specially crafted files in various formats such as X_B, DWG, DXF, STL, STP, SLDPRT and PAR format. If a user is tricked to open a malicious file with the affected applications, an attacker could leverage the vulnerability to crash the application, extract data or potentially lead to arbitrary code execution.

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
Solid Edge SE2022: All versions < V222.0MP12	Update to V222.0MP12 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Solid Edge SE2022: All versions only affected by CVE-2022-46345, CVE-2022-46346, CVE-2022-46347, CVE-2022-46348, CVE-2022-46349, CVE-2023-22295, CVE-2023-22321, CVE-2023-22354, CVE-2023-22669, CVE-2023-22670, CVE-2023-22846, CVE-2023-23579, CVE-2023-24564, CVE-2023-24565, CVE-2023-24566, CVE-2023-24581	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Solid Edge SE2023: All versions < V223.0Update2 only affected by CVE-2022-46345, CVE-2022-46346, CVE-2022-46347, CVE-2022-46348, CVE-2022-46349, CVE-2023-22295, CVE-2023-22321, CVE-2023-22354, CVE-2023-22669, CVE-2023-22670, CVE-2023-22846, CVE-2023-23579, CVE-2023-24549, CVE-2023-24550, CVE-2023-24551, CVE-2023-24552, CVE-2023-24553, CVE-2023-24554, CVE-2023-24555, CVE-2023-24556, CVE-2023-24557, CVE-2023-24558, CVE-2023-24559, CVE-2023-24560, CVE-2023-24561, CVE-2023-24562, CVE-2023-24563, CVE-2023-24564, CVE-2023-24565, CVE-2023-24566, CVE-2023-24581	Update to V223.0Update2 or later version https://support.sw.siemens.com/ 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:

- Do not open untrusted X_B, DWG, DXF, STL, STP, SLDPRT and PAR files 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-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, ZDI-CAN-19072)

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, ZDI-CAN-19073)

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-2021-32948

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-19074, 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-2021-43336

Open Design Alliance Drawings SDK before 2022.11 used in affected products contains an out of bounds write vulnerability when parsing a DXF file. An attacker can leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15107, ZDI-CAN-19080, ZDI-CAN-19075)

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-2021-43391

Open Design Alliance Drawings SDK before 2022.11 used in affected products contains an out of bounds write vulnerability when parsing a DXF file. An attacker can leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19082)

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-2022-46345

The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19070)

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-2022-46346

The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19071)

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-2022-46347

The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19079)

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-2022-46348

The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19383)

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-2022-46349

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19384)

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-2023-22295

Datakit CrossCadWare_x64.dll used in affected products contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19448)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-22321

Datakit CrossCadWare_x64.dll used in affected products contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19501)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-22354

Datakit CrossCadWare_x64.dll used in affected products contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19424)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-22669

Open Design Alliance Drawings SDK used in affected application is vulnerable to heap-based buffer 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 while parsing specially crafted DWG 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-2023-22846

Datakit CrossCadWare_x64.dll used in affected products contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19473)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-23579

Datakit CrossCadWare_x64.dll used in affected products contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SLDPRT file. This could allow an attacker to to execute code in the context of the current process. (ZDI-CAN-19423)

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-2023-24549

The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could 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-121: Stack-based Buffer Overflow

Vulnerability CVE-2023-24550

The affected application is vulnerable to heap-based buffer while parsing specially crafted PAR files. An attacker could 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-24551

The affected application is vulnerable to heap-based buffer underflow while parsing specially crafted PAR files. An attacker could 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-24552

The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to 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-2023-24553

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24554

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24555

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24556

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24557

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24558

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24559

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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-2023-24560

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to 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-2023-24561

The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could 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-824: Access of Uninitialized Pointer

Vulnerability CVE-2023-24562

The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could 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-824: Access of Uninitialized Pointer

Vulnerability CVE-2023-24563

The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could 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-824: Access of Uninitialized Pointer

Vulnerability CVE-2023-24564

The affected application contains a memory corruption vulnerability while parsing specially crafted DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19069)

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2023-24565

The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted STL file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19428)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-24566

The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19472)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2023-24581

The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted STP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19425)

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-2023-25140

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. 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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of vulnerabilities from CVE-2023-24549 to CVE-2023-24563 and CVE-2023-25140
- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2023-24564, CVE-2023-22670, CVE-2022-46348, CVE-2022-46345, CVE-2022-46346, CVE-2022-46349, CVE-2022-46347, CVE-2023-24565, CVE-2023-24566, CVE-2023-23579, CVE-2023-22354, CVE-2023-22295, CVE-2023-22321 and CVE-2023-22846
- Open Design Alliance for coordination efforts of CVE-2021-43336, CVE-2021-32938, CVE-2021-32948, CVE-2021-43391, CVE-2021-32936, CVE-2023-22669 and CVE-2023-22670

ADDITIONAL INFORMATION

This advisory covers security vulnerabilities (CVE-2023-23579, CVE-2023-22354, CVE-2023-22295, CVE-2023-22846, and CVE-2023-22321) in CrossCadWare_x64 library of Datakit [1].

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK (CVE-2023-22670, CVE-2023-22669) refer [2].

[1] CrossCad/Ware - OEM integration of reading and writing libraries and dlls for software editors: https://www.datakit.com/en/crosscad_ware.php

[2] 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 (2023-02-14): Publication Date
V1.1 (2023-03-14): Correction in version formats of fixes

TERMS OF USE