SSA-728618: Multiple Vulnerabilities in Solid Edge before SE2021MP8

Publication Date: 2021-09-28
Last Update: 2021-09-28
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released a new version for Solid Edge that fixes multiple file parsing vulnerabilities which could be triggered when the application reads files in IFC, JT or OBJ formats.

If a user is tricked to opening a malicious file using the affected application this could lead the application to crash, or potentially arbitrary code execution on the target host system.

Siemens recommends to update to the latest version and to limit opening of files from unknown sources in the affected products.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2021: All versions < SE2021MP8	Update to SE2021MP8 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Avoid opening files from unknown sources in Solid Edge

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-2021-37202

The IFC adapter in affected application contains a use-after-free vulnerability that could be triggered while parsing user-supplied IFC 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-416: Use After Free

Vulnerability CVE-2021-37203

The plmxmlAdapterIFC.dll contains an out-of-bounds read while parsing user supplied IFC files which could result in a read past the end of an allocated buffer. This could allow an attacker to cause a denial-of-service condition or read sensitive information from memory locations.

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-2021-41533

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files.

An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565).

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:T/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-41534

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files.

An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703).

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:T/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-41535

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771).

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:T/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-41536

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778).

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:T/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-41537

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789).

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:T/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-41538

The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files.

An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770).

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:T/RC:C
CWE	CWE-824: Access of Uninitialized Pointer

Vulnerability CVE-2021-41539

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773).

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:T/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-41540

The affected application contains a use-after-free vulnerability while parsing OBJ files.

An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13776).

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:T/RC:C
CWE	CWE-416: Use After Free

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- xina1i for reporting vulnerabilities CVE-2021-37202 and CVE-2021-37203
- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2021-41533 through CVE-2021-41540

ADDITIONAL INFORMATION

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 (2021-09-28): Publication Date

TERMS OF USE