SSA-818688: Multiple Vulnerabilities in Solid Edge before SE2021MP7

Publication Date: 2021-08-10
Last Update: 2021-08-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released a new version for Solid Edge that fixes three vulnerabilities - an XML external entity (XXE) injection, and two file parsing issues which could be triggered when the application reads OBJ files.

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 and data extraction 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 < SE2021MP7	Update to SE2021MP7 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-2021-37178

An XML external entity injection vulnerability in the underlying XML parser could cause the affected application to disclose arbitrary files to remote attackers by loading a specially crafted xml file.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

Vulnerability CVE-2021-37179

The PSKERNEL.dll library in affected application lacks proper validation while parsing user-supplied OBJ files that could lead to a use-after-free condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13777)

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-2021-37180

The PSKERNEL.dll library lacks proper validation while parsing user-supplied OBJ files that could cause an out of bounds access to an uninitialized pointer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13775)

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-824: Access of Uninitialized Pointer

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

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 (2021-08-10):   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.