SSA-572164: Luxion KeyShot Vulnerability in Solid Edge

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

The Solid Edge installation package includes a specific version of the third-party product KeyShot from Luxion : https://www.keyshot.com, which may not contain the latest security fixes provided by Luxion.

Siemens recommends to update KeyShot according to the information in the Luxion Security Advisory LSA-610622: https://download.keyshot.com/cert/lsa-610622/lsa-610622.pdf.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2023: All versions	Update KeyShot 11 (as bundled with SE2023) to KeyShot V2023.1 or later version https://www.keyshot.com/resources/downloads/ 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

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.

 © Siemens 2023

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-2021-27044

KeyShot's FBX importer `luxion_geometry_fbx.exe` uses Autodesk FBX Review version 1.4.0 which consists of an out of bounds read/write vulnerability. This may allow an attacker to execute arbitrary code or lead to information disclosure. (ZDI-CAN-18490)

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

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Luxion for coordination efforts

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in Luxion KeyShot, refer to:

- Luxion Security Advisory LSA-610622: https://download.keyshot.com/cert/lsa-610622/lsa-610622.pdf
- AutoDesk Advisory ADSK-SA-2021-0001: https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0001

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 (2023-04-11): 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.