SSA-231216: Luxion KeyShot Vulnerabilities in Solid Edge

Publication Date: 2021-03-09
Last Update: 2021-03-09
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, 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-192169.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2020: All versions	Update KeyShot V8 (as bundled with SE2020) to V10.1 or later version https://www.keyshot.com/resources/downloads/
Solid Edge SE2021: All versions	Update KeyShot V9 (as bundled with SE2021) to V10.1 or later version https://www.keyshot.com/resources/downloads/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow 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-2021-22643

Importing of malicious 3DS file would cause out-of-bounds read and crash KeyShot's 3DS importer luxion_geometry_3ds.exe. It may allow an attacker to execute arbitrary code. (ZDI-CAN-11938, ZDI-CAN-11939)

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-2021-22645

KeyShot project files (.bip) were prone to malicious load instructions when KeyShot opened such a file. Such instructions were able to load a DLL through a remote network share, and run its entry point function. (ZDI-CAN-11940)

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-357: Insufficient UI Warning of Dangerous Operations

Vulnerability CVE-2021-22647

Importing of malicious 3DS and FBX file would cause out-of-bounds write and crash KeyShot's 3DS or FBX importer luxion_geometry_3ds.exe. It may allow an attacker to execute arbitrary code. (ZDI-CAN-11941, ZDI-CAN-11944, ZDI-CAN-11946, ZDI-CAN-11984).

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-2021-22649

Importing of malicious 3DS and JT file would cause untrusted pointer dereference and crash KeyShot's Datakit importer luxion_geometry_3ds.exe. It may allow an attacker to execute arbitrary code. (ZDI-CAN-11942, ZDI-CAN-12064)

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-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-22651

Importing of malicious Creo files (ZIP archives with extensions: edz, pyc, or c3di) would cause path traversal: extracting files that would end up outside of the destination directory hierarchy. Files placed in such a fashion could be able to run as scripts during system startup. (ZDI-CAN-11983)

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-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Luxion for coordination efforts

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in Luxion KeyShot before V10.1, refer to:

- Luxion Security Advisory LSA-192169

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 (2021-03-09): Publication Date

TERMS OF USE