SSA-119468: Luxion KeyShot Vulnerabilities in Solid Edge

Publication Date: 2021-05-25
Last Update: 2021-05-25
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-394129.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2020: All versions	Update KeyShot V8 (as bundled with SE2020) to V10.2 or later version https://www.keyshot.com/resources/downloads/
Solid Edge SE2021: All versions	Update KeyShot V9 (as bundled with SE2021) to V10.2 or later version https://www.keyshot.com/resources/downloads/

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

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-2021-27488

Affected applications lack proper validation of user-supplied data when parsing of CATPart files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-11950).

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-2021-27492

When opening a specially crafted 3DXML file, the application could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underlying XML parser without taking proper restrictions such as prohibiting an external dtd (ZDI-CAN-11952).

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

Vulnerability CVE-2021-27494

Affected applications lack proper validation of user-supplied data when parsing of STP files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-11953).

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:U/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2021-27496

Affected applications lack proper validation of user-supplied data when parsing PRT files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-11962).

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:U/RC:C
CWE	CWE-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-27490

The affected products are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code (ZDI-CAN-12084).

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Luxion for coordination efforts
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

ADDITIONAL INFORMATION

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

- Luxion Security Advisory LSA-394129
- ICS Advisory ICSA-21-145-01

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 (2021-05-25): Publication Date

TERMS OF USE