LSA-610622: Vulnerability discovered in FBX SDK used in KeyShot

- Publication Date: 2023-03-14
- Last Update: 2023-03-14
- Current Version: 1.0
- CVSS v3.1 Base Score: 7.8

Summary

Trend Micro's Zero Day Initiative (ZDI) discovered and disclosed a vulnerability pertaining to Autodesk FBX SDK 2020.0.1 and before, which is used by Luxion software:

- CVE-2021-27044 (ZDI-CAN-18490)

More information at: https://www.zerodayinitiative.com/advisories/published/

Luxion has mitigated for the vulnerability in KeyShot 2023.1 by updating from Autodesk FBX SDK 2020.2.1 to 2020.3.2. The vulnerability was fixed in 2020.2.2, as per ADSK-SA-2021-0001, but the recommendation was to upgrade to 2020.3.2.

Affected Products and Remediation

- KeyShot
    - Affected versions: All versions before 2023.1
    - Remediation: Upgrade to version 2023.1 or later

Product Description

KeyShot is a photo-realistic real-time rendering program with a scene structure that can be setup and manipulated for rendering. It allows import of various CAD formats into its scene structure.

Vulnerability Classification

Classification of the vulnerabilities has been done by using CVSS 3.1 (https://nvd.nist.gov/vuln-metrics/cvss/) with additional CWE classification (https://cwe.mitre.org/).

Importing of malicious FBX file would cause heap-based buffer overflow via KeyShot's FBX importer `luxion_geometry_fbx.exe`. It may allow an attacker to execute arbitrary code.

- CVE-2021-27044
- 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
- CWE-125: Out-of-bounds Read
- CWE-787: Out-of-bounds Write

Acknowledgments

Luxion thanks the following parties for their efforts:

- Autodesk for coordination efforts and fixing vulnerability in bundled libraries (ADSK-SA-2021-0001)
- Siemens for coordination efforts
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

Additional Information

Further details about Luxion CSIRT and advisories can be found at: https://www.keyshot.com/csirt/

History Data

v1.0 (2023-03-14): Publication date

Terms of Use

Luxion security advisories are subject to the terms and conditions contained in the license terms or other applicable agreement previously made with Luxion. To the extent applicable to information, software or documentation made available in or by a Luxion security advisory, the "Terms of Use" of Luxion global website shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.