KSA-655925: Vulnerabilities discovered in third party libraries and KeyShot Studio

- Publication Date: 2024-11-12
- Last Update: 2024-11-22
- Current Version: 1.1
- CVSS v3.1 Base Score: 7.8

Summary

Trend Micro's Zero Day Initiative (ZDI) discovered and disclosed 5 vulnerabilities pertaining to third party libriares, which is used by KeyShot software, and 1 vulnerability pertaining to KeyShot software directly:

- ZDI-CAN-23681
- ZDI-CAN-23685
- ZDI-CAN-23693
- ZDI-CAN-23697
- ZDI-CAN-23700
- ZDI-CAN-23826

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

KeyShot has mitigated for the vulnerabilities in version 2024.3.

Affected Products and Remediation

- KeyShot Studio
  - Affected versions: All versions before 2024.2
  - Remediation: Upgrade to version 2024.3 or later

Product Description

KeyShot Studio 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://www.first.org/cvss/) with additional CWE classification (https://cwe.mitre.org/).

- Vulnerability ZDI-CAN-23681

  Parsing of malicious 3DS file would cause heap-based buffer overflow via KeyShot's 3DS importer `luxion_geometry_3ds.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11576
  - 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-122: Heap-based buffer overflow

- Vulnerability ZDI-CAN-23685

  Parsing of malicious SKP file would cause out-of-bounds write via KeyShot's Sketchup importer `luxion_geometry_sketchup.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11577

  - 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-787: Out-of-bounds write

- Vulnerability ZDI-CAN-23693

  Parsing of malicious 3DS file would cause stack-based buffer overflow via KeyShot's 3DS importer `luxion_geometry_3ds.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11578
  - 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-121: Heap-based buffer overflow

- Vulnerability ZDI-CAN-23697

  Parsing of malicious OBJ file would cause out-of-bounds write via KeyShot's OBJ importer `luxion_geometry_obj.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11579
  - 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-787: Out-of-bounds write

- Vulnerability ZDI-CAN-23700

  Parsing of malicious ABC file would cause heap-based buffer overflow via KeyShot's Alembic importer `luxion_geometry_alembic.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11580
  - 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-122: Heap-based buffer overflow

- Vulnerability ZDI-CAN-23826

  Importing of malicious JT file would cause out-of-bounds read via KeyShot's Datakit importer `luxion_geometry.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2024-11581
  - 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

Acknowledgments

KeyShot thanks the following parties for their efforts:

- Zero Day Initiative for coordinated disclosure

Additional Information

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

History Data

v1.0 (2024-11-12): Publication date v1.1 (2024-11-22): CVEs assigned

Terms of Use

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