KSA-113962: Vulnerabilities discovered in KeyShot Studio

- Publication Date: 2025-03-11
- Last Update: 2025-03-11
- Current Version: 1.0
- CVSS v3.1 Base Score: 7.8

Summary

Trend Micro's Zero Day Initiative (ZDI) discovered and disclosed 3 vulnerabilities pertaining to KeyShot software:

- ZDI-CAN-23646
- ZDI-CAN-23694
- ZDI-CAN-24586

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

KeyShot has mitigated for the vulnerabilities in version 2025.1.

Affected Products and Remediation

- KeyShot Studio
  - Affected versions: All versions before 2025.1
  - Remediation: Upgrade to version 2025.1 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-23646

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

  - CVE-2025-1046
  - 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-416: Use after free

- Vulnerability ZDI-CAN-23694

  Parsing of malicious PVS file would access uninitialized pointer via KeyShot's PTC importer `luxion_geometry_dapi.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2025-1047
  - 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-457: Use of Uninitialized Variable

- Vulnerability ZDI-CAN-24586

  Parsing of malicious KSP/BIP file would cause a head-based buffer overflow in KeyShot. It may allow an attacker to execute arbitrary code.

  - CVE-2025-1045
  - 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

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 (2025-03-11): Publication date

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.