LSA-563106: Vulnerabilities reported by Zero Day Initiative

- Publication Date: 2024-03-12
- Last Update: 2024-03-12
- Current Version: 1.0
- CVSS v3.1 Base Score: 7.8

Summary

Simon Janz (@esj4y) and Sean de Regge, working with Trend Micro Zero Day Initiative (ZDI), discovered and disclosed four vulnerabilities pertaining to Luxion software products:

- ZDI-CAN-22266
- ZDI-CAN-22267
- ZDI-CAN-22514
- ZDI-CAN-22738

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

Luxion has mitigated for the vulnerabilities in version 2024.1.

Affected Products and Remediation

- KeyShot
  - Affected versions: All versions before 2024.1
  - Remediation: Upgrade to version 2024.1 or later
- KeyShot Viewer
  - Affected versions: All versions before 2024.1
  - Remediation: Upgrade to version 2024.1 or later
- KeyShot Network Rendering
  - Affected versions: All versions before 2024.1
  - Remediation: Upgrade to version 2024.1 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.

KeyShot Viewer is a read-only version of KeyShot in which scenes can only be viewed and rendered, but not manipulated or exported.

KeyShot Network Rendering is a product that enables for efficient rendering of KeyShot scenes in cooperation of many other computers in a network.

Vulnerability Classification

Classification of the vulnerability has been done by using CVSS 3.1 (https://www.first.org/cvss/) with additional CWE classification (https://cwe.mitre.org/).

- Vulnerabilities ZDI-CAN-22266 and ZDI-CAN-22267
  - Opening of malicious KeyShot project files (.ksp, .bip) could cause out-of-bounds write and potentially remote code execution.
    - CVSS v3.1 base score: 7.8
– CWE-20: Improper Input Validation

• Vulnerability ZDI-CAN-22514

  Opening of malicious KeyShot project files (.ksp, .bip) could cause infinite recursion, leading to out-of-bounds write and potentially remote code execution.
  
  – CVSS v3.1 base score: 7.8
  – CWE-665: Improper Initialization

• Vulnerability ZDI-CAN-22738

  Opening of malicious KeyShot project files (.ksp, .bip) could result in a DLL planting attack via incorrect search paths fallback, and potentially remote code execution.
  
  – CVSS v3.1 base score: 7.8
  – CWE-427: Uncontrolled Search Path Element

Acknowledgments

Luxion thanks the following parties for their efforts:

• Zero Day Initiative for coordinated disclosure

Additional Information

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

History Data

v1.0 (2024-03-12): 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.