LSA-192169: Vulnerabilities reported by Zero Day Initiative

- Publication Date: 2021-02-04
- Last Update: 2021-02-04
- Current Version: 1.0
- CVSS v3.1 Base Score: 7.8

Summary

Trend Micro's Zero Day Initiative (ZDI) discovered and disclosed 11 vulnerabilities pertaining to Luxion software products:

- ZDI-CAN-11938
- ZDI-CAN-11939
- ZDI-CAN-11940
- ZDI-CAN-11941
- ZDI-CAN-11942
- ZDI-CAN-11944
- ZDI-CAN-11946
- ZDI-CAN-11948
- ZDI-CAN-11983
- ZDI-CAN-11984
- ZDI-CAN-12064

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

Luxion has mitigated for the vulnerabilities in version 10.1.

Affected Products and Remediation

- KeyShot
  - Affected versions: All versions before 10.1
  - Remediation: Upgrade to version 10.1 or later
- KeyShot Viewer
  - Affected versions: All versions before 10.1
  - Remediation: Upgrade to version 10.1 or later
- KeyShot Network Rendering
  - Affected versions: All versions before 10.1
  - Remediation: Upgrade to version 10.1 or later
- KeyVR
  - Affected versions: All versions before 10.1
  - Remediation: Upgrade to version 10.1 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.

KeyVR is a product that enables KeyShot scenes to be immersively experienced via VR headsets, and in collaboration with others through network connectivity.

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/).

- Vulnerabilities ZDI-CAN-11938, ZDI-CAN-11939

  Importing of malicious 3DS file would cause out-of-bounds read and crash KeyShot's 3DS importer `luxion_geometry_3ds.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2021-22643
  - 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

- Vulnerability ZDI-CAN-11940

  KeyShot project files (.bip) were prone to malicious `load` instructions when KeyShot opened such a file. Such instructions were able to load a DLL through a remote network share, and run its entry point function.

  - CVE-2021-22645
  - 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-357: Insufficient UI warning of dangerous operations

- Vulnerability ZDI-CAN-11941

  Importing of malicious 3DS file would cause out-of-bounds write and crash KeyShot's 3DS importer `luxion_geometry_3ds.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2021-22647
  - 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-11942

  Importing of malicious 3DS file would cause untrusted pointer dereference and crash KeyShot's 3DS importer `luxion_geometry_3ds.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2021-22649
  - 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-822: Untrusted pointer dereference

- Vulnerability ZDI-CAN-11944, ZDI-CAN-11946, ZDI-CAN-11984

  Importing of malicious FBX file would cause out-of-bounds write and crash KeyShot's FBX importer `luxion_geometry_fbx.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2021-22647
  - 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-11948

  Importing of malicious CATPart file would cause out-of-bounds write and crash KeyShot's Datakit importer `luxion_geometry.exe`. It may allow an attacker to execute arbitrary code.

  - 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-11983

  Importing of malicious Creo files (ZIP archives with extensions: edz, pyc, or c3di) would cause path traversal: extracting files that would end up outside of the destination directory hierarchy. Files placed in such a fashion could be able to run as scripts during system startup.

  - CVE-2021-22651
  - 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-22: Improper limitation of a path name to a restricted directory ("path traversal")

- Vulnerability ZDI-CAN-12064

  Importing of malicious JT file would cause untrusted pointer dereference and crash KeyShot's Datakit importer `luxion_geometry.exe`. It may allow an attacker to execute arbitrary code.

  - CVE-2021-22649
  - 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-822: Untrusted pointer dereference

Acknowledgments

Luxion thanks the following parties for their efforts:

- Zero Day Initiative for coordinated disclosure
- Industrial Control Systems Vulnerability Management and Coordination (ICS-VMC) for coordination efforts
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) 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 (2021-02-04): Publication date

Terms of Use

