LSA-394129: Vulnerabilities discovered in Datakit used in KeyShot

- Publication Date: 2021-05-25
- Last Update: 2021-05-25
- Current Version: 1.0
- CVSS v3.1 Base Score: 7.8

Summary

Trend Micro's Zero Day Initiative (ZDI) discovered and disclosed 5 vulnerabilities pertaining to Datakit 2021.1 and before, which is used by Luxion software:

- CVE-2021-27488 (ZDI-CAN-11950)
- CVE-2021-27492 (ZDI-CAN-11952)
- CVE-2021-27494 (ZDI-CAN-11953)
- CVE-2021-27496 (ZDI-CAN-11962)
- CVE-2021-27490 (ZDI-CAN-12084)

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

Luxion has mitigated for the vulnerabilities in version 10.2.

Affected Products and Remediation

- KeyShot
  - Affected versions: All versions before 10.2
  - Remediation: Upgrade to version 10.2 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://www.first.org/cvss/) with additional CWE classification (https://cwe.mitre.org/).

- Vulnerability CVE-2021-27488 (ZDI-CAN-11950)

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

  - CVE-2021-27488
  - 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 CVE-2021-27492 (ZDI-CAN-11952)

  Importing of malicious 3DXML file would cause information disclosure due to processing of XML external entity via KeyShot's Datakit importer `luxion_geometry.exe`.

  - CVE-2021-27492
  - CVSS v3.1 base score: 5.5
  - CVSS vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

  - CWE-611: Improper restriction of XML external entity reference

- Vulnerability CVE-2021-27494 (ZDI-CAN-11953)

  Importing of malicious STP file would cause buffer overflow when parsing via KeyShot's Datakit importer `luxion_geometry.exe`. It may allow an attacker to execute code arbitrary code.

  - CVE-2021-27494
  - 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: Stack-based buffer overflow

- Vulnerability CVE-2021-27496 (ZDI-CAN-11962)

  Importing of malicious PRT file would cause untrusted pointer derefence via KeyShot's Datakit importer `luxion_geometry.exe`. It may allow an attacker to execute code arbitrary code.

  - CVE-2021-27496
  - 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 CVE-2021-27490 (ZDI-CAN-12084)

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

  - CVE-2021-27490
  - 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

Luxion thanks the following parties for their efforts:

- Datakit CrossCADWare for coordination efforts and fixing vulnerabilities in bundled libraries
- 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 (2021-05-25): Publication date

Terms of Use

