ADVISORY DETAILS

March 20th, 2025

(0Day) Luxion KeyShot DAE File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

ZDI-25-174
ZDI-CAN-23704

CVE ID	CVE-2025-2531
CVSS SCORE	7.8, AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
AFFECTED VENDORS	Luxion
AFFECTED PRODUCTS	KeyShot
VULNERABILITY DETAILS	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of dae files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.
ADDITIONAL DETAILS	09/11/24 – ZDI reported the vulnerability to the vendor 09/25/24 – the vendor acknowledged the receipt of the report

01/06/25 – the vendor requested an extension until March 2025
02/11/25 - ZDI asked for updates
02/19/25 – the vendor requested an extension until June 2025
02/19/25 - ZDI notified the vendor of the intention to publish the case as a 0-day advisory

DISCLOSURE TIMELINE

2024-09-11 - Vulnerability reported to vendor
2025-03-20 - Coordinated public release of advisory
2025-03-20 - Advisory Updated

CREDIT

Anonymous

< BACK TO ADVISORIES

General Inquiries
zdi@trendmicro.com

Find us on X
@thezdi

Find us on Mastodon
Mastodon

Media Inquiries
media_relations@trendmicro.com

Sensitive Email Communications
PGP Key