

ADVISORY DETAILS

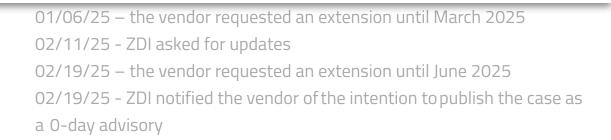
March 20th, 2025

(ODay) Luxion KeyShot DAE File Parsing Access of Uninitialized Pointer Remote Code Execution Vulnerability

ZDI-25-173 ZDI-CAN-23698

CVE ID	CVE-2025-2530
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 initialization of a pointer prior to accessing it. 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





~

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.con Sensitive Email Co PGP Key	_	Find us on Mastodon Mastodon	Media Inquiries media_relations@trendmicro.com
WHO WE ARE Our Mission Trend Micro TippingPoint IPS	HOW IT WORKS Process Researcher Rewards FAQS Privacy	ADVISORIES Published Advisories Upcoming Advisories RSS Feeds	BLOG



