ADVISORY DETAILS
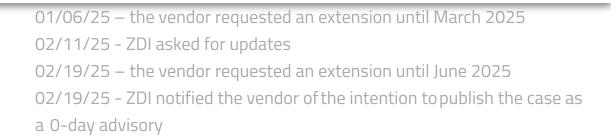
March 20th, 2025

(0Day) Luxion KeyShot USDC File Parsing Use-After-Free Remote Code Execution Vulnerability

ZDI-25-175
ZDI-CAN-23709

CVE ID	CVE-2025-2532
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 usdc files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. 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**

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