ZK Framework AuUploader Unspecified Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-36537
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-26 20:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	ZK Framework v9.6.1, 9.6.0.1, 9.5.1.3, 9.0.1.2 and 8.6.4.1 allows attackers to access sensitive information via a crafted PO

Risk And Classification

EPSS: 0.939420000 probability, percentile 0.998850000 (date 2026-05-12)

CISA KEV: Listed on 2023-02-27; due 2023-03-20; ransomware use Known

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	ZK Framework
Product	AuUploader
Name	ZK Framework AuUploader Unspecified Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://tracker.zkoss.org/browse/ZK-5150; https://nvd.nist.gov/vuln/detail/CVE-2022-36537

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zkoss	Zk Framework	All	All	All	All
Application	Zkoss	Zk Framework	8.6.4.1	All	All	All
Application	Zkoss	Zk Framework	9.0.1.2	All	All	All
Application	Zkoss	Zk Framework	9.5.1.3	All	All	All
Application	Zkoss	Zk Framework	9.6.0.1	All	All	All
Application	Zkoss	Zk Framework	9.6.1	All	All	All

References

Reference	Source	Link	Tags
[ZK-5150] Vulnerability in zk upload - ZK-Tracker	MISC	tracker.zkoss.org	
CISA warns of hackers exploiting ZK Java Framework RCE flaw	MISC	www.bleepingcomputer.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150657 ZK Framework - Authentication Bypass Vulnerability (CVE-2022-36537)

378061 ConnectWise R1Soft Server Backup Manager Improper Neutralization Vulnerability