CVE-2026-31238

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

Summary

CVE	CVE-2026-31238
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:16:52 UTC
Updated	2026-05-13 15:47:35 UTC
Description	The Ludwig framework thru 0.10.4 is vulnerable to insecure deserialization (CWE-502) in its model serving component. Wh

Risk And Classification

EPSS: 0.000200000 probability, percentile 0.058640000 (date 2026-05-13)

Problem Types: n/a

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
github.com/ludwig-ai/ludwig	cve@mitre.org	github.com	
www.notion.so/CVE-2026-31238-35d1e1393188819ea77ee98ca85a2878	cve@mitre.org	www.notion.so	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report