



CVE-2023-43791

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-43791
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-09 15:15:00 UTC
Updated	2023-11-18 00:55:00 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Humansignal	Label Studio	All	All	All	All

References

Reference
Release 1.8.2 · HumanSignal/label-studio · GitHub
Hardcoded Django `SECRET_KEY` that can be Abused to Forge Session Tokens · Advisory · HumanSignal/label-studio · GitHub
fix: LSDV-5071: Ensure secret key is securely set persisting a new one if required by bmartel · Pull Request #4690 · HumanSignal/label-studio · GitHub
fix: LSDV-5071: Ensure secret key is securely set persisting a new on... · HumanSignal/label-studio@3d06c51 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995874](#) Python (Pip) Security Update for label-studio (GHSA-f475-x83m-rx5m)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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