



CVE-2023-36472

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-36472
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-15 19:15:00 UTC
Updated	2023-09-21 13:57:00 UTC
Description	Strapi is an open-source headless content management system. Prior to version 4.11.7, an unauthorized actor can get acc

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strapi	Strapi	All	All	All	All

References

Reference	Source	L
Leaking sensitive user information, user reset password, tokens via content-manager views · Advisory · strapi/strapi · GitHub	MISC	g
Release v4.11.7 · strapi/strapi · GitHub	MISC	g
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995281](#) NodeJs (Npm) Security Update for @strapi/admin (GHSA-v8gg-4mq2-88q4)

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