



CVE-2022-30617

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

Summary

CVE	CVE-2022-30617
State	PUBLIC
Assigner	disclosure@synopsys.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-19 18:15:00 UTC
Updated	2022-06-06 15:51:00 UTC
Description	An authenticated user with access to the Strapi admin panel can view private and sensitive data, such as email and password.

Risk And Classification

Problem Types: CWE-212

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strapi	Strapi	All	All	All	All
Application	Strapi	Strapi	4.0.0	beta10	All	All
Application	Strapi	Strapi	4.0.0	beta11	All	All
Application	Strapi	Strapi	4.0.0	beta12	All	All
Application	Strapi	Strapi	4.0.0	beta13	All	All
Application	Strapi	Strapi	4.0.0	beta14	All	All
Application	Strapi	Strapi	4.0.0	beta15	All	All
Application	Strapi	Strapi	4.0.0	beta2	All	All
Application	Strapi	Strapi	4.0.0	beta3	All	All
Application	Strapi	Strapi	4.0.0	beta4	All	All
Application	Strapi	Strapi	4.0.0	beta5	All	All
Application	Strapi	Strapi	4.0.0	beta6	All	All
Application	Strapi	Strapi	4.0.0	beta7	All	All
Application	Strapi	Strapi	4.0.0	beta8	All	All
Application	Strapi	Strapi	4.0.0	beta9	All	All

References

Reference	Source	Link
CyRC Vulnerability Advisory: Sensitive data exposure in JSON enables account compromise in Strapi Synopsys	MISC	www.synopsys.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). 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