



CVE-2023-46240

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

Summary

CVE	CVE-2023-46240
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-31 16:15:00 UTC
Updated	2023-11-08 23:43:00 UTC
Description	CodeIgniter is a PHP full-stack web framework. Prior to CodeIgniter4 version 4.4.3, if an error or exception occurs, a detailed

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Error Handling — CodeIgniter 4.3.2 documentation	MISC	codeigniter4.github
Merge pull request from GHSA-hwxj-qxj7-7rfj · codeigniter4/CodeIgniter4@423569f · GitHub	MISC	github.com
Detailed Error Report is Displayed in Production Environment · Advisory · codeigniter4/CodeIgniter4 · GitHub	MISC	github.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.

Legacy QID Mappings

[995767](#) PHP (Composer) Security Update for codeigniter4/framework (GHSA-hwxj-qxj7-7rfj)

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](#)