



CVE-2021-39175

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

Summary

CVE	CVE-2021-39175
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-30 21:15:00 UTC
Updated	2022-10-25 18:01:00 UTC
Description	HedgeDoc is a platform to write and share markdown. In versions prior to 1.9.0, an unauthenticated attacker can inject arbitrary HTML into the rendered output.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Disable GA and Disqus in default CSP by davidmehren · Pull Request #1375 · hedgedoc/hedgedoc · GitHub	MISC	github.com	
Remove unsafe-eval from default CSP by davidmehren · Pull Request #1369 · hedgedoc/hedgedoc · GitHub	MISC	github.com	
XSS vector in slide mode speaker-view · Advisory · hedgedoc/hedgedoc · GitHub	CONFIRM	github.com	
Tighten up Content-Security-Policy by davidmehren · Pull Request #1513 · hedgedoc/hedgedoc · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	cc
NVD vulnerability detail	NVD	nvd.nist.gov	cc

No vendor comments have been submitted for this CVE.

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

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