



CVE-2021-21422

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

Summary

CVE	CVE-2021-21422
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-21 19:15:00 UTC
Updated	2021-06-29 14:02:00 UTC
Description	mongo-express is a web-based MongoDB admin interface, written with Node.js and express. 1: As mentioned in this issue:

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mongo-express Project	Mongo-express	1.0.0	alpha1	All	All
Application	Mongo-express Project	Mongo-express	1.0.0	alpha3	All	All
Application	Mongo-express Project	Mongo-express	All	All	All	All

References

Reference	Source	Link
HTML in String fields is not escaped if only preview is loaded · Issue #577 · mongo-express/mongo-express · GitHub	MISC	github.co
Merge pull request from GHSA-7p8h-86p5-wv3p · mongo-express/mongo-express@f5e0d49 · GitHub	MISC	github.co
Multiple XSS Vulnerabilities · Advisory · mongo-express/mongo-express · GitHub	CONFIRM	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982047](#) Nodejs (npm) Security Update for mongo-express (GHSA-7p8h-86p5-wv3p)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)