



CVE-2022-25297

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

Summary

CVE	CVE-2022-25297
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-21 08:15:00 UTC
Updated	2022-02-28 19:22:00 UTC
Description	This affects the package drogonframework/drogon before 1.7.5. The unsafe handling of file names during upload using Http

Risk And Classification

Problem Types: CWE-552

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Lin
Prevent malformed upload path causing arbitrary write by Kirill89 · Pull Request #1174 · drogonframework/drogon · GitHub	CONFIRM	gith
Prevent malformed upload path causing arbitrary write (#1174) · drogonframework/drogon@3c78532 · GitHub	CONFIRM	gith
Arbitrary File Write in drogonframework/drogon CVE-2022-25297 Snyk	CONFIRM	sny
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

Vendor Comments And Credit

Discovery Credit

LEGACY: Snyk Security Team

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](#) 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](#)