



CVE-2022-32177

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

Summary

CVE	CVE-2022-32177
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-14 07:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3beta are vulnerable to Unrestricted File Upload that leads to execution o

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gin-vue-admin Project	Gin-vue-admin	2.5.3	beta	All	All
Application	Gin-vue-admin Project	Gin-vue-admin	All	All	All	All

References

Reference	Source	Link	Tags
gin-vue-admin/common.vue at v2.5.3beta · flipped-aurora/gin-vue-admin · GitHub	CONFIRM	github.com	
CVE-2022-32177 Mend Vulnerability Database	MISC	www.mend.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Mend Vulnerability Research Team (MVR)

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

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