



CVE-2021-25956

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

Summary

CVE	CVE-2021-25956
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-17 15:15:00 UTC
Updated	2022-11-17 17:21:00 UTC
Description	In "Dolibarr" application, v3.3.beta1_20121221 to v13.0.2 have "Modify" access for admin level users to change other user's

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dolibarr	Dolibarr	3.3.0	beta1	All	All
Application	Dolibarr	Dolibarr	3.3.0	beta2	All	All
Application	Dolibarr	Dolibarr	All	All	All	All
Application	Dolibarr	Dolibarr Erp/crm	3.3.0	beta1	All	All
Application	Dolibarr	Dolibarr Erp/crm	3.3.0	beta2	All	All

References

Reference	Source	Link	Ta
CVE-2021-25956 WhiteSource Vulnerability Database	MISC	www.whitesourcesoftware.com	
FIX Broken Access Control reported by Ahsan Aziz. · Dolibarr/dolibarr@c4cba43 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

LEGACY: Daniel Elkabes

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](#).

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