CVE-2020-14209

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-14209
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-02 17:15:00 UTC
Updated	2021-03-30 14:37:00 UTC
Description	Dolibarr before 11.0.5 allows low-privilege users to upload files of dangerous types, leading to arbitrary code execution. Thi

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Dolibarr ERP/CRM 11.0.4 Bypass / Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
wizlynx group | Unrestricted Upload of File with Dangerous Type in Dolibarr ERP/CRM	MISC	www.wizlynxgroup.com	Third Party
Release 11.0.5 · Dolibarr/dolibarr · GitHub	CONFIRM	github.com	Release No
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report