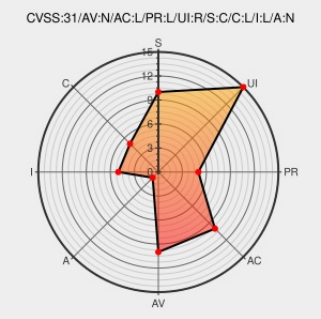
CVE-2020-13094

Published on: 05/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:43 PM UTC

CVE-2020-13094

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dolibarr from Dolibarr contain the following vulnerability:

Dolibarr before 11.0.4 allows XSS.

CVE-2020-13094 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
dolibarr/ChangeLog at 11.0.4 · Dolibarr/dolibarr · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/Dolibarr/dolibarr/blob/11.0.4/ChangeLog

Dolibarr 11.0.3 Cross Site Scripting ≈ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/157752/Dolibarr-11.0.3-Cross-Site-Scripting.html
Dolibarr ERP CRM 11.0.4 (maintenance release for branch 11.0) is available	Release Notes Vendor Advisory www.dolibarr.org text/html	MISC www.dolibarr.org/dolibarr-erp-crm-11-0-4-maintenance-release-for-branch-11-0-is-available.php

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Dolibarr 11.0.3 - Persistent Cross-Site Scripting

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:dolibarr:dolibarr:*:*:*:*:*:*:*:*:

cpe:2.3:a:dolibarr:dolibarr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→