



CVE-2019-14330

Published on: 07/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:58 PM UTC

CVE-2019-14330

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Espocrm](#) from [Espocrm](#) contain the following vulnerability:

An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create Case. A malicious attacker can modify the firstName and lastName to contain JavaScript code.

CVE-2019-14330 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
xss fixes · espocrm/espocrm@4ab7d19 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/espocrm/espocrm/commit/4ab7d19776011288b875abd3eef1e1f6f75289e2

EspoCrm 5

Exploit

Third Party Advisory

www.cinquino.eu

text/html

MISC www.cinquino.eu/EspoCRM.htm

Comparing 5.6.5...5.6.6 · espocrm/espocrm · GitHub

Third Party Advisory

github.com

text/html

MISC github.com/espocrm/espocrm/compare/5.6.5...5.6.6

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:espocrm:espocrm:*****:

cpe:2.3:a:espocrm:espocrm:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→