



CVE-2019-10074

Published on: 09/11/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-10074

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

An RCE is possible by entering Freemarker markup in an Apache OFBiz Form Widget textarea field when encoding has been disabled on such a field. This was the case for the Customer Request "story" input in the Order Manager application. Encoding should not be disabled without good reason and never within a field that accepts user

input. Mitigation: Upgrade to 16.11.06 or manually apply the following commit on branch 16.11: r1858533

CVE-2019-10074 has been assigned by security@apache.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Apache** - **OFBiz** version **OFBiz 16.11.01 to 16.11.05**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description

Tags

Link

Pony Mail!

Mailing List

Vendor Advisory

lists.apache.org

text/html

MLIST [ofbiz-notifications] 20190913 [jira] [Updated] (OFBIZ-11006) Create customer request screen breaks when entering special characters (CVE-2019-10074)

Pony Mail!

Mailing List

Vendor Advisory

s.apache.org

text/html

MLIST [ofbiz-dev] 20190910 [CVE-2019-10074] Apache OFBiz RCE (template injection)

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	Apache	Ofbiz	All	All	All	All
cpe:2.3:a:apache:ofbiz:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→