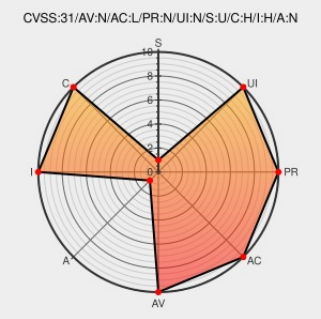
CVE-2021-23128

Published on: 03/04/2021 12:00:00 AM UTC

Last Modified on: 12/22/2022 12:08:01 PM UTC

CVE-2021-23128

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



Certain versions of Joomla! from Joomla contain the following vulnerability:

An issue was discovered in Joomla! 3.2.0 through 3.9.24. The core shipped but unused randval implementation within FOF (FOFEncryptRandval) used an potential insecure implemetation. That has now been replaced with a call to 'random_bytes()' and its backport that is shipped within random_compat.

CVE-2021-23128 has been assigned by security@joomla.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Joomla! Project** - **Joomla! CMS** version **= 3.2.0-3.9.24**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
[20210302] - Core - Potential Insecure	Vendor Advisory	MISC developer.joomla.org/security-centre/842-20210302-core-

FOFEncryptRandval developer.joomla.org potential-insecure-fofencryptrandval.html text/html

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.

Related QID Numbers

11999 Joomla Core Multiple Vulnerabilities(20210305, 20210302, 20210301)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Joomla!	All	All	All	All
Application	Joomla	Joomla!	All	All	All	All

cpe:2.3:a:joomla:joomla\!:*:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→