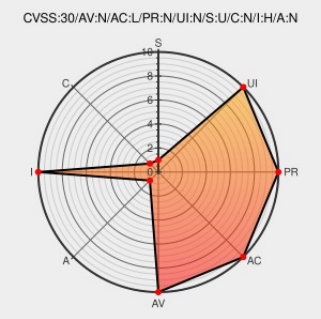
CVE-2016-9838

Published on: 12/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9838

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



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

An issue was discovered in components/com_users/models/registration.php in Joomla! before 3.6.5. Incorrect filtering of registration form data stored to the session on a validation error enables a user to gain access to a registered user's account and reset the user's group mappings, username, and password, as demonstrated by submitting a form that targets the `registration.register` task.

CVE-2016-9838 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Joomla! 3.6.5 Released	Patch, Vendor Advisory	CONFIRM www.joomla.org/announcements/release-news/5693-joomla-3-6-5-released.html

	www.joomla.org text/html	
Joomla! < 3.6.4 - Admin Takeover - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 41157
Joomla! Core CVE-2016-9838 Remote Privilege Escalation Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94893

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

Exploit/POC from Github

cve-2016-9838

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→