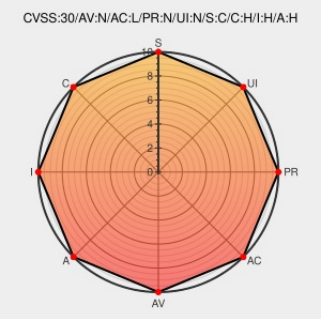
CVE-2019-3809

Published on: 03/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:42 PM UTC

CVE-2019-3809

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



Certain versions of Moodle from Moodle contain the following vulnerability:

A flaw was found in Moodle versions 3.1 to 3.1.15 and earlier unsupported versions. The mybackpack functionality allowed setting the URL of badges, when it should be restricted to the Mozilla Open Badges backpack URL. This resulted in the possibility of blind SSRF via requests made by the page.

CVE-2019-3809 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **[UNKNOWN]** - **moodle** version **3.1.16**

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	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
Official Moodle git projects - moodle.git/search	Patch	CONFIRM git.moodle.org/gw?

	Vendor Advisory git.moodle.org text/xml	p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-64222
1668067 – (CVE-2019-3809) CVE-2019-3809 moodle: Blind SSRF Risk in /badges/mybackpack.php (MSA-19-0002)	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3809
Moodle.org: MSA-19-0002: Blind SSRF Risk in /badges/mybackpack.php	Patch Vendor Advisory moodle.org text/html	CONFIRM moodle.org/mod/forum/discuss.php?d=381229#p1536766

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:moodle:moodle:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→