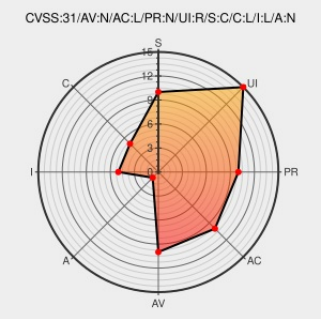
CVE-2019-3810

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

Last Modified on: 11/07/2022 07:02:00 PM UTC

CVE-2019-3810

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 3.6 to 3.6.1, 3.5 to 3.5.3, 3.4 to 3.4.6, 3.1 to 3.1.15 and earlier unsupported versions. The /userpix/ page did not escape users' full names, which are included as text when hovering over profile images. Note this page is not linked to by default and its access is restricted.

CVE-2019-3810 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **[UNKNOWN]** - **moodle** version **3.6.2**

Affected Vendor/Software: **[UNKNOWN]** - **moodle** version **3.5.4**

Affected Vendor/Software: **[UNKNOWN]** - **moodle** version **3.4.7**

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

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
Official Moodle git projects - moodle.git/search	Patch Vendor Advisory git.moodle.org text/xml	CONFIRM git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-64372
Moodle.org: MSA-19-0003: User full name is not escaped in the un-linked userpix page	Patch Vendor Advisory moodle.org text/html	CONFIRM moodle.org/mod/forum/discuss.php?d=381230#p1536767
1668073 – (CVE-2019-3810) CVE-2019-3810 moodle: User full name is not escaped in the un-linked userpix page (MSA-19-0003)	Issue Tracking Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3810
Moodle 3.6.1 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162399/Moodle-3.6.1-Cross-Site-Scripting.html

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Moodle (< 3.6.2, < 3.5.4, < 3.4.7, < 3.1.16) XSS PoC for Privilege Escalation (Student to Admin)

Known Affected Configurations (CPE V2.3)

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@pwnwikiorg	CVE-2019-3810 Moodle 3.6.1 XSS漏洞 pwnwiki.org/index.php?titl…	2021-04-30 10:14:51
@BlogLoki	【PoC】CVE-2019-3810 ・企業でも利用されている案件管理ソフトにおけるXSSのPoC exploit-db.com/exploits/49814	2021-04-30 11:29:18
@LinInfoSec	Moodle - CVE-2019-3810: moodle.org/mod/forum/disc…	2021-05-05 16:56:21

← Previous ID

Next ID→