



# LearnDash LMS <= 4.6.0 - Authenticated (Subscriber+) Insecure Direct Object Reference to Arbitrary User Password Change

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-3105
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-12 05:15:10 UTC
<b>Updated</b>	2026-04-08 17:16:59 UTC
<b>Description</b>	The LearnDash LMS plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and includi

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from security@wordfence.com

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Problem Types:** CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	StellarWP	LearnDash LMS	affected 4.6.0 semver	Not specified

### References

Reference	Source
www.learndash.com/release-notes	af854a3a-210
LearnDash LMS <= 4.6.0 - Authenticated (Subscriber+) Insecure Direct Object Reference to Arbitrary User Password Change	af854a3a-210
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

### Vendor Comments And Credit

Discovery Credit

**CNA:** István Márton (en)

### Additional Advisory Data

Source	Time	Event
CNA	2023-06-05T00:00:00.000Z	Discovered
CNA	2023-06-05T00:00:00.000Z	Vendor Notified
CNA	2023-06-27T00:00:00.000Z	Disclosed

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)