



# LearnDash LMS <= 4.10.1 - Sensitive Information Exposure via API

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2024-1210   |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Wordfence   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2024-02-05 22:16:08 UTC   |
| <b>Updated</b>         | 2026-04-08 18:20:30 UTC   |
| <b>Description</b>     | The LearnDash LMS plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including |

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

| Version | Source                 | Type      | Score | Severity | Vector                                       |
|---------|------------------------|-----------|-------|----------|--|
| 3.1     | nvd@nist.gov           | Primary   | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 3.1     | security@wordfence.com | Secondary | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 3.1     | CNA                    | DECLARED  | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**Low**

Low

Integrity

None

Availability

None

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

### 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 4.10.1 semver | Not specified |

### References

| Reference  | Source                               | Link   |
|--|--------------------------------------|--|
| www.learndash.com/release-notes  | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.learndash.com/release-notes">www.learndash.com/release-notes</a>   |
| github.com/karlemilnikka/CVE-2024-1208-and-CVE-2024-1210                           | af854a3a-2127-422b-91ae-364da2661108 | <a href="https://github.com/karlemilnikka/CVE-2024-1208-and-CVE-2024-1210">github.com/karlemilnikka/CVE-2024-1208-and-CVE-2024-1210</a>  |
| www.wordfence.com/threat-intel/vulnerabilities/id/61ca5ab6-5fe9-4313-9b0d-87366... | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/61ca5ab6-5fe9-4313-9b0d-87366...">www.wordfence.com/threat-intel/vulnerabilities/id/61ca5ab6-5fe9-4313-9b0d-87366...</a> |
| CVE Program record   | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>   |
| NVD vulnerability detail   | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>   |

### Vendor Comments And Credit

Discovery Credit

**CNA:** Karl Emil Nikka (en)

### Additional Advisory Data

| Source | Time                     | Event           |
|--------|--------------------------|-----------------|
| CNA    | 2023-12-25T00:00:00.000Z | Vendor Notified |
| CNA    | 2024-02-02T00:00:00.000Z | Disclosed       |

### Legacy QID Mappings

731200 LearnDash LMS plugin for WordPress Insufficient Information Vulnerability

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)