Security Advisory 2024-085

Multiple Vulnerabilities in Moodle

August 21, 2024 — v1.0

TLP:CLEAR

History:

- *21/08/2024 — v1.0 – Initial publication*

Summary

On August 19, 2024, Moodle released a security advisory addressing sixteen vulnerabilities of various severities [1,2].

It is recommended updating as soon as possible.

Technical Details

Several CVEs have been assigned with a *Serious* severity or risk by Moodle.

The vulnerability **CVE-2024-43440** is a Local File Inclusion (LFI) flaw triggered when restoring malformed block backups [3].

The vulnerability **CVE-2024-43439** is a flaw in unsanitised H5P error messages allowing for Reflected Cross-Site Scripting (XSS) [4].

The vulnerability **CVE-2024-43436** is an SQL injection flaw in the XMLDB editor tool available to site administrators [5].

The vulnerability **CVE-2024-43434** is a flaw in the bulk message sending feature for the feedback module's non-respondents report due to an incorrect CSRF token check, and possibly leading to Cross-Site Request Forgery (CSRF) [6].

The vulnerability **CVE-2024-43431** is an Insecure Direct Object Reference (IDOR) flaw that allows users to delete badges they do not have permission to access due to insufficient capability checks [7].

The vulnerability **CVE-2024-43428** is a cache poisoning flaw due to insufficient validation of local storage, allowing injection into the storage mechanism [8].

The vulnerability **CVE-2024-43426** is a serious arbitrary file read flaw due to insufficient sanitisation in the TeX notation filter, affecting sites where pdfTeX is available [9].

The vulnerability **CVE-2024-43425** is a remote code execution flaw through calculated question types [10].

Affected Products

The following Moodle versions are affected by the vulnerabilities:

- 4.4 to 4.4.1;
- 4.3 to 4.3.5;
- 4.2 to 4.2.8;
- 4.1 to 4.1.11;
- Earlier unsupported versions.

Recommendations

It is recommended updating affected assets as soon as possible.

References

[1] https://moodle.org/security/index.php

[2] https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0696/

[3] https://moodle.org/mod/forum/discuss.php?d=461209#p1851881

[4] https://moodle.org/mod/forum/discuss.php?d=461209#p1851881

[5] https://moodle.org/mod/forum/discuss.php?d=461206#p1851878

[6] https://moodle.org/mod/forum/discuss.php?d=461203#p1851874

[7] https://moodle.org/mod/forum/discuss.php?d=461199#p1851870

[8] https://moodle.org/mod/forum/discuss.php?d=461196#p1851867

[9] https://moodle.org/mod/forum/discuss.php?d=461194#p1851864

[10] https://moodle.org/mod/forum/discuss.php?d=461193#p1851861