CVE-2022-35653

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-35653
State	PUBLIC
Assigner	patrick@puiterwijk.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-25 16:15:00 UTC
Updated	2023-11-07 03:49:00 UTC
Description	A reflected XSS issue was identified in the LTI module of Moodle. The vulnerability exists due to insufficient sanitization of u

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Moodle	Moodle	All	All	All	All
Application	Moodle	Moodle	4.0.0	-	All	All
Application	Moodle	Moodle	4.0.0	beta	All	All
Application	Moodle	Moodle	4.0.0	rc1	All	All
Application	Moodle	Moodle	4.0.0	rc2	All	All
Application	Moodle	Moodle	4.0.0	rc3	All	All
Application	Moodle	Moodle	4.0.0	rc4	All	All
Application	Moodle	Moodle	4.0.1	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference
[SECURITY] Fedora 35 Update: moodle-3.11.8-1.fc35 - package-announce - Fedora Mailing-Lists
2106277 – (CVE-2022-35653, MSA-22-0019) CVE-2022-35653 moodle: LTI module reflected XSS risk - affecting unauthenticated users only
[SECURITY] Fedora 35 Update: moodle-3.11.8-1.fc35 - package-announce - Fedora Mailing-Lists

Moodle.org: MSA-22-0019: LTI module reflected XSS risk - affecting unauthenticated users only
[SECURITY] Fedora 36 Update: moodle-3.11.8-1.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 36 Update: moodle-3.11.8-1.fc36 - package-announce - Fedora Mailing-Lists
Official Moodle git projects - moodle.git/search
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

282973 Fedora Security Update for moodle (FEDORA-2022-81ce74b2dd)

282974 Fedora Security Update for moodle (FEDORA-2022-7e7ce7df2e)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**