



CVE-2022-40313

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

Summary

CVE	CVE-2022-40313
State	PUBLIC
Assigner	patrick@puiterwijk.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-30 17:15:00 UTC
Updated	2022-12-21 15:01:00 UTC
Description	Recursive rendering of Mustache template helpers containing user input could, in some cases, result in an XSS risk or a pa

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Moodle	Moodle	All	All	All	All

References

Reference

- [Moodle.org: MSA-22-0023: Stored XSS and page denial of service risks due to recursive rendering in Mustache template helpers](#)
- [2128146 – \(CVE-2022-40313\) CVE-2022-40313 moodle: Stored XSS and page denial of service risks due to recursive rendering in Mustache](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[283130](#) Fedora Security Update for moodle (FEDORA-2022-50c091d963)

[283131](#) Fedora Security Update for moodle (FEDORA-2022-1c77803b43)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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