



CVE-2023-45818

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

Summary

CVE	CVE-2023-45818
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-19 22:15:00 UTC
Updated	2023-10-26 16:32:00 UTC
Description	TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCE

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tiny	Tinymce	All	All	All	All

References

Reference	Score
tinymce.html.SaxParser Docs TinyMCE	MI
mXSS vulnerability in TinyMCE undo/redo, getContent API, resetContent API, and Autosave plugin · Advisory · tinymce/tinymce · GitHub	MI
TinyMCE 6.7.1 TinyMCE Documentation	MI
Just a moment...	MI
TinyMCE 5.10.8 Docs TinyMCE	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995617](#) PHP (Composer) Security Update for tinymce/tinymce (GHSA-v65r-p3vv-jjfv)

[995657](#) NodeJs (Npm) Security Update for tinymce (GHSA-v65r-p3vv-jjfv)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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