



CVE-2021-23639

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

Summary

CVE	CVE-2021-23639
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-10 20:15:00 UTC
Updated	2021-12-14 18:48:00 UTC
Description	The package md-to-pdf before 5.0.0 are vulnerable to Remote Code Execution (RCE) due to utilizing the library gray-matter

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Markdown To Pdf Project	Markdown To Pdf	All	All	All	All

References

Reference
Security: gray-matter exposes front matter JS-engine that leads to arbitrary code execution · Issue #99 · simonhaenisch/md-to-pdf · GitHub
fix: disable JS engine for front-matter by default to prevent RCE · simonhaenisch/md-to-pdf@a716259 · GitHub
Remote Code Execution (RCE) in md-to-pdf Snyk
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit
LEGACY: Oscar Arnflo

There are currently no legacy QID mappings associated with this CVE.

© [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](#)