



CVE-2022-35144

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

Summary

CVE	CVE-2022-35144
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-04 20:15:00 UTC
Updated	2022-08-11 14:10:00 UTC
Description	Renato v0.17.0 was discovered to contain a cross-site scripting (XSS) vulnerability.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Raneto Project	Raneto	All	All	All	All

References

Reference
Releases · gilbitron/Raneto · GitHub
CWE - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (4.12)
Raneto - A free, open, simple Markdown powered Knowledgebase for Nodejs
CVE-2022-35142, CVE-2022-35143, CVE-2022-35144 - DoS, XSS and Weak Password Policy in Renato a Markdown powered knowledge ba
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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