



CVE-2022-25020

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

Summary

CVE	CVE-2022-25020
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-01 02:15:00 UTC
Updated	2022-03-09 00:47:00 UTC
Description	A cross-site scripting (XSS) vulnerability in Pluxml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a cr

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pluxml	Pluxml	5.8.7	All	All	All

References

Reference	Source	Link	Tags
DOM-based and Stored XSS Vulnerability in PluXml - YouTube	MISC	youtu.be	
CVE-2022-25020/CVE-2022-25020.pdf at main · MoritzHuppert/CVE-2022-25020 · GitHub	MISC	github.com	
CVE-2021-38602 : PluXML 5.8.7 allows Article Editing stored XSS via Headline or Content.	MISC	www.cvedetails.com	
Accueil - PluXml.org	MISC	pluxml.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

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

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](#)