



CVE-2020-28707

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

Summary

CVE	CVE-2020-28707
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-19 22:15:00 UTC
Updated	2021-01-22 21:42:00 UTC
Description	The Stockdio Historical Chart plugin before 2.8.1 for WordPress is affected by Cross Site Scripting (XSS) via stockdio_char

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Stockdio	Stockdio Historical Chart	All	All	All	All
Application	Stockdio	Stockdio Historical Chart	All	All	All	All

References

Reference	Source	Link	Tags
jondow CVE-2020-28707 – XSS in Stockdio Historical Chart plugin for WordPress before version 2.8.1	MISC	jondow.eu	Explo
Stockdio Historical Chart – WordPress plugin WordPress.org	CONFIRM	wordpress.org	Relea
Stockdio - From Zero to Financial Market Analytics in less than 60 seconds!	MISC	stockdio.com	Vend
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

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