CVE-2019-20209

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-20209
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-13 18:15:00 UTC
Updated	2020-01-14 15:35:00 UTC
Description	The CTHthemes CityBook before 2.3.4, TownHub before 1.0.6, and EasyBook before 1.2.2 themes for WordPress allow ns

Risk And Classification

Problem Types: CWE-79 | CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cththemes	Citybook	All	All	All	All
Application	Cththemes	Citybook	All	All	All	All
Application	Cththemes	Easybook	All	All	All	All
Application	Cththemes	Easybook	All	All	All	All
Application	Cththemes	Townhub	All	All	All	All
Application	Cththemes	Townhub	All	All	All	All

References

Reference	Source	Link	Tags
EasyBook < 1.2.2 - Multiple Vulnerabilities	MISC	wpvulndb.com	Third Par
TownHub < 1.0.6 - Multiple Vulnerabilities	MISC	wpvulndb.com	Third Par
TownHub - Directory & Listing WordPress Theme v1.0.2 Multiple Vulnerabilities - CXSecurity.com	MISC	cxsecurity.com	Exploit, T
CityBook - Directory & Listing WordPress Theme v2.2.2 Multiple Vulnerabilities - CXSecurity.com	MISC	cxsecurity.com	Exploit, T
CityBook - Directory & Listing WordPress Theme by cththemes | ThemeForest	MISC	themeforest.net	Third Par
CityBook < 2.3.4 - Multiple Vulnerabilities	MISC	wpvulndb.com	Third Par
EasyBook – Directory & Listing WordPress Theme by cththemes | ThemeForest	MISC	themeforest.net	Third Par
EasyBook – Directory & Listing WordPress Theme v1.2.1 Multiple Vulnerabilities - CXSecurity.com	MISC	cxsecurity.com	Exploit, T

TownHub - Directory & Listing WordPress Theme by cththemes | ThemeForest	MISC	themeforest.net	Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report