



CVE-2020-12800

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

Summary

CVE	CVE-2020-12800
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 17:15:00 UTC
Updated	2020-06-11 00:36:00 UTC
Description	The drag-and-drop-multiple-file-upload-contact-form-7 plugin before 1.3.3.3 for WordPress allows Unrestricted File Upload

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codedropz	Drag And Drop Multiple File Upload - Contact Form 7	All	All	All	All
Application	Codedropz	Drag And Drop Multiple File Upload - Contact Form 7	All	All	All	All

References

Reference	Source	Link	Tags
WordPress Drag And Drop Multi File Uploader Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit,
Drag and Drop Multiple File Upload – Contact Form 7 – WordPress plugin WordPress.org	CONFIRM	wordpress.org	Release
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

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