



CVE-2023-26852

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-26852
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-12 17:15:00 UTC
Updated	2023-04-21 03:51:00 UTC
Description	An arbitrary file upload vulnerability in the upload plugin of Textpattern v4.8.8 and below allows attackers to execute arbitra

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Textpattern	Textpattern	All	All	All	All

References

Reference

- Update your browser to use Google Drive, Docs, Sheets, Sites, Slides, and Forms - Google Drive Help
- GitHub - textpattern/textpattern: A flexible, elegant, fast and easy-to-use content management system written in PHP.
- GitHub - leekenghwa/CVE-2023-26852-Textpattern-v4.8.8-and-: Textpattern v4.8.8 and Below are vulnerable to Unrestricted File Upload Leac
- 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.

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