



CVE-2021-44082

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

Summary

CVE	CVE-2021-44082
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-29 23:15:00 UTC
Updated	2022-04-06 18:41:00 UTC
Description	textpattern 4.8.7 is vulnerable to Cross Site Scripting (XSS) via /textpattern/index.php,Body. A remote and unauthenticated

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Textpattern	Textpattern	4.8.7	All	All	All

References

Reference	Source	Link	Tags
Leveraging XSS to get RCE in Textpattern Pentest Limited	MISC	pentest.co.uk	
Infosec	MISC	www.cornerpirate.com	
Pentest Limited Information Security Assurance	MISC	www.pentest.co.uk	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730415](#) Textpattern CMS Cross-Site Scripting (XSS) Vulnerability

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