



CVE-2022-27852

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

Summary

CVE	CVE-2022-27852
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-15 17:15:00 UTC
Updated	2023-11-07 03:45:00 UTC
Description	Multiple Unauthenticated Stored Cross-Site Scripting (XSS) vulnerabilities in KB Support (WordPress plugin) <= 1.5.5 versio

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpchill	Kb Support	All	All	All	All

References

Reference

- WordPress KB Support – WordPress Help Desk plugin <= 1.5.5 - Multiple Unauthenticated Stored Cross-Site Scripting (XSS) vulnerabilities -
- WordPress KB Support plugin <= 1.5.5 - Multiple Unauth. Stored Cross-Site Scripting (XSS) vulnerabilities - Patchstack
- KB Support – WordPress Help Desk – WordPress plugin | WordPress.org
- 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