



CVE-2022-43146

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

Summary

CVE	CVE-2022-43146
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-14 21:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	An arbitrary file upload vulnerability in the image upload function of Canteen Management System v1.0 allows attackers to e

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canteen Management System Project	Canteen Management System	1.0	All	All	All

References

Reference	Source	Link
Canteen Management System Project Source Code in PHP Free Download Free Source Code Projects and Tutorials	MISC	www.s...
CVE-2022-43146: RCE via Arbitrary File Upload by Syedmudassiruddinalvi Nov, 2022 Medium		mediu...
CVE-2022-43146: RCE via Arbitrary File Upload by Syedmudassiruddinalvi Nov, 2022 Medium	MISC	mediu...
CVE Program record	CVE.ORG	www.c...
NVD vulnerability detail	NVD	nvd.nis...

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