



CVE-2022-30930

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

Summary

CVE	CVE-2022-30930
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-14 17:15:00 UTC
Updated	2023-12-22 15:15:00 UTC
Description	Tourism Management System Version: V 3.2 is affected by: Cross Site Request Forgery (CSRF).

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpgurukul	Tourism Management System	3.2	All	All	All
Application	Tourism Management System Project	Tourism Management System	3.2	All	All	All

References

Reference	Source	Link
My second CVE-2022-30930. Cross-Site Request Forgery (CSRF) on... by Praveen Mali (PMMALI) Medium		medium.com
My second CVE-2022-30930. Cross-Site Request Forgery (CSRF) on... by Praveen Mali Jun, 2022 Medium	MISC	medium.com
Possible CSRF (Cross-site request forgery) - Vulnerabilities - Acunetix	MISC	www.acunetix.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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