



CVE-2020-35745

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

Summary

CVE	CVE-2020-35745
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-07 21:15:00 UTC
Updated	2024-02-01 02:22:00 UTC
Description	PHPGURUKUL Hospital Management System V 4.0 does not properly restrict access to admin/dashboard.php, which allow

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpgurukul	Hospital Management System	4.0	All	All	All
Application	Phpgurukul	Hospital Management System In Php	4.0	All	All	All
Application	Phpgurukul	Hospital Management System In Php	4.0	All	All	All

References

Reference	Source	L
Privilege Escalation - Unauthenticated access to Admin Portal (CVE-2020-35745) - YouTube	MISC	v
Hospital Management System In PHP - PHPGurukul	MISC	v
Privilege Escalation — Unauthenticated access to Admin Portal (CVE-2020-35745) by Ashish Dhone Jan, 2021 Medium	MISC	r
Privilege Escalation — Unauthenticated access to Admin Portal (CVE-2020-35745) by Ashish Dhone Jan, 2021 Medium		r
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)