



CVE-2023-1950

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

Summary

CVE	CVE-2023-1950
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-08 08:15:00 UTC
Updated	2023-12-21 04:01:00 UTC
Description	A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. Affected by

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bp Monitoring Management System Project	Bp Monitoring Management System	1.0	All	All	All
Application	Phpgurukul	Bp Monitoring Management System	1.0	All	All	All

References

Reference

[vuldb.com](#)

[BP-Monitoring-Management-System/password-recovery.php_SQL_English.pdf at main · vsdwef/BP-Monitoring-Management-System · GitHub](#)

[CVE-2023-1950 | PHPGurukul BP Monitoring Management System Password Recovery password-recovery.php sql injection](#)

[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.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report