



CVE-2022-0813

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

Summary

CVE	CVE-2022-0813
State	PUBLIC
Assigner	cve-coordination@incibe.es
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-10 17:44:00 UTC
Updated	2023-11-26 12:15:00 UTC
Description	PhpMyAdmin 5.1.1 and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. TI

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpmyadmin	Phpmyadmin	All	All	All	All

References

Reference	Source	Link	Tags
PhpMyAdmin exposure of sensitive information INCIBE-CERT	CONFIRM	www.incibe-cert.es	
phpMyAdmin: Multiple Vulnerabilities (GLSA 202311-17) — Gentoo security		security.gentoo.org	
phpMyAdmin - phpMyAdmin 4.9.10 and 5.1.3 are released	CONFIRM	www.phpmyadmin.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Rafael Pedrero

Legacy QID Mappings

150518 phpMyAdmin Information Exposure Vulnerability (CVE-2022-0813)

183486 Debian Security Update for phpmyadmin (CVE-2022-0813)

710799 Gentoo Linux phpMyAdmin Multiple Vulnerabilities (GLSA 202311-17)

730632 PhpMyAdmin Information Disclosure Vulnerability

© [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](#)