



CVE-2016-9866

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-9866
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-11 03:00:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	An issue was discovered in phpMyAdmin. When the arg_separator is different from its default & value, the CSRF token was

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.002220000 probability, percentile 0.446240000 (date 2026-05-07)

Problem Types: CWE-352 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpmyadmin	Phpmyadmin	4.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.14	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.15	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.16	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.17	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.5	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.0.10.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.14	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.14.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.3	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.4.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.4	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References		
Reference	Source	Link
phpMyAdmin PMASA-2016-71 Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
phpMyAdmin - Security - PMASA-2016-71	af854a3a-2127-422b-91ae-364da2661108	www.phpmyadmin.com
phpMyAdmin: Multiple vulnerabilities (GLSA 201701-32) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings
501149 Alpine Linux Security Update for phpmyadmin
505232 Alpine Linux Security Update for phpmyadmin
710467 Gentoo Linux Hypertext Preprocessor (PHP) MyAdmin Multiple Vulnerabilities (GLSA 201701-32)

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