



CVE-2016-6611

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

Summary

CVE	CVE-2016-6611
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-11 02:59:17 UTC
Updated	2026-05-06 22:30:45 UTC
Description	An issue was discovered in phpMyAdmin. A specially crafted database and/or table name can be used to trigger an SQL inj

Risk And Classification

Primary CVSS: v3.0 8.1 HIGH from nvd@nist.gov

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

EPSS: 0.003650000 probability, percentile 0.585490000 (date 2026-05-09)

Problem Types: CWE-89 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:H/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	4.0.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc3	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	4.0.10.2	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	4.4.14.1	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	4.4.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.4	All	All	All

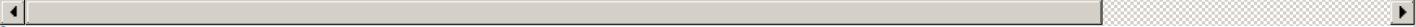
Application	Phpmyadmin	Phpmyadmin	4.4.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	alpha1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc2	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

Vendor Declared Affected Products

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

References

Reference	Source	Link
phpMyAdmin - Security - PMASA-2016-34	af854a3a-2127-422b-91ae-364da2661108	www.phpmyadmin
[SECURITY] [DLA 1821-1] phpmyadmin security update	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
phpMyAdmin CVE-2016-6611 SQL-Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus
phpMyAdmin: Multiple vulnerabilities (GLSA 201701-32) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.or
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

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