



# CVE-2016-9857

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

## Summary

|                 |                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-9857                                                                                                        |
| State           | PUBLISHED                                                                                                            |
| Assigner        | mitre                                                                                                                |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                         |
| Published       | 2016-12-11 02:59:56 UTC                                                                                              |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                              |
| Description     | An issue was discovered in phpMyAdmin. XSS is possible because of a weakness in a regular expression used in some Ja |

## Risk And Classification

**Primary CVSS:** v3.0 6.1 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.004180000 probability, percentile 0.618680000 (date 2026-05-09)

**Problem Types:** CWE-79 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 6.1   | MEDIUM   | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N |
| 2.0     | nvd@nist.gov | Primary | 4.3   |          | AV:N/AC:M/Au:N/C:N/I:P/A:N                   |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Low

Availability

None

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



CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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



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

|             |                            |                            |         |     |     |     |
|-------------|----------------------------|----------------------------|---------|-----|-----|-----|
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.4   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.5   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.6   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.6.1 | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.7   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.8   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.4.9   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.6.0   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.6.1   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.6.2   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.6.3   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 4.6.4   | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |
|-----------------------------------|--------------------|---------------------|--------------|---------------|
| Source                            | Vendor             | Product             | Version      | Platforms     |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

| References                                                              |                                      |                                       |
|-------------------------------------------------------------------------|--------------------------------------|---------------------------------------|
| Reference                                                               | Source                               | Link                                  |
| phpMyAdmin PMASA-2016-64 Multiple Cross Site Scripting Vulnerabilities  | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.securityfocus.com</a> |
| phpMyAdmin - Security - PMASA-2016-64                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.phpmyadmin.net</a>    |
| phpMyAdmin: Multiple vulnerabilities (GLSA 201701-32) — Gentoo security | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">security.gentoo.org</a>   |
| CVE Program record                                                      | CVE.ORG                              | <a href="#">www.cve.org</a>           |
| NVD vulnerability detail                                                | NVD                                  | <a href="#">nvd.nist.gov</a>          |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings                                                                                                |
|--------------------------------------------------------------------------------------------------------------------|
| <a href="#">501149</a> Alpine Linux Security Update for phpmyadmin                                                 |
| <a href="#">505232</a> Alpine Linux Security Update for phpmyadmin                                                 |
| <a href="#">710467</a> 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)