



CVE-2010-3056

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

Summary

CVE	CVE-2010-3056
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-08-24 20:00:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 2.11.x before 2.11.10.1 and 3.x before 3.3.5.1 allow remot

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

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	Phpmysqladmin	Phpmysqladmin	2.11.0	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.11.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.10.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.7.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.7.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.8.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.11.9.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	alpha	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	beta	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.2	rc1	All	All

Application	Phpmyadmin	Phpmyadmin	3.1.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.5.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
phpMyAdmin Multiple Cross Site Scripting Vulnerabilities	af854a3a-2127-422b-91ae-364da2661100
[SECURITY] Fedora 13 Update: phpMyAdmin-3.3.5.1-1.fc13	af854a3a-2127-422b-91ae-364da2661100
phpMyAdmin Cross-Site Scripting Vulnerabilities - Advisories - Community	af854a3a-2127-422b-91ae-364da2661100
phpMyAdmin - Security - PMASA-2010-5	af854a3a-2127-422b-91ae-364da2661100
Bug 625877 – CVE-2010-3056 phpMyAdmin: several XSS vulnerabilities fixed in 3.3.5.1/2.11.10.1	af854a3a-2127-422b-91ae-364da2661100
Debian -- Security Information -- DSA-2097-1 phpmyadmin	af854a3a-2127-422b-91ae-364da2661100
yehg.net/lab/pr0js/advisories/phpmyadmin/%5Bphpmyadmin-3.3.5%5D_cross_...	af854a3a-2127-422b-91ae-364da2661100
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661100

Support / Security / Advisories // MDVSA-2010:163 Mandriva	af854a3a-2127-422b-91ae-364da266110
Debian update for phpmyadmin - Advisories - Community	af854a3a-2127-422b-91ae-364da266110
Webmail - OVH	af854a3a-2127-422b-91ae-364da266110
[SECURITY] Fedora 12 Update: phpMyAdmin-3.3.5.1-1.fc12	af854a3a-2127-422b-91ae-364da266110
Support / Security / Advisories // MDVSA-2010:164 Mandriva	af854a3a-2127-422b-91ae-364da266110
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)