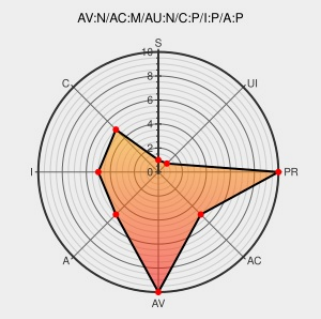
CVE-2004-1055

Published on: 11/24/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1055

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux from Gentoo contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 2.6.0-pl2 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the PmaAbsoluteUri parameter, (2) the zero_rows parameter in read_dump.php, (3) the confirm form, or (4) an error message generated by the internal phpMyAdmin parser.

CVE-2004-1055 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
phpMyAdmin > Security | MySQL Database Administration Tool | www.phpmyadmin.net	Exploit, www.phpmyadmin.net, text/html	CONFIRM www.phpmyadmin.net/home_page/security.php?issue=PMASA-2004-3
404 Not Found	Exploit, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.netvigilance.com/html/advisory0005.htm
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF phpmyadmin-multiple-xss(18158)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	rc1	All	All
Operating System	Gentoo	Linux	1.4	rc2	All	All
Operating System	Gentoo	Linux	1.4	rc3	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	rc1	All	All
Operating System	Gentoo	Linux	1.4	rc2	All	All
Operating System	Gentoo	Linux	1.4	rc3	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl2	All	All	All

cpe:2.3:o:gentoo:linux:1.4:*:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc1:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc2:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc3:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:*:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc1:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc2:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:1.4:rc3:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.0:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc2:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2024 | |
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 registred 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