



CVE-2007-4255

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

Summary

CVE	CVE-2007-4255
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-08 23:17:00 UTC
Updated	2018-10-15 21:34:00 UTC
Description	Buffer overflow in the mSQL extension in PHP 5.2.3 allows context-dependent attackers to execute arbitrary code via a long

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.3	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
PHP mSQL (mysql_connect) - Local Buffer Overflow (PoC) - Multiple dos Exploit	EXPLOIT-DB	www.exploit-db.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
PHP MSQL_Connect Buffer Overflow Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-08-09	Joshua Bressers	Not vulnerable. PHP packages as shipped with Red Hat Enterprise Linux versions 2.1, 3, 4,

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](#)