



# CVE-2015-5723

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-5723
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-06-07 14:06:00 UTC
<b>Updated</b>	2023-11-07 02:26:00 UTC
<b>Description</b>	Doctrine Annotations before 1.2.7, Cache before 1.3.2 and 1.4.x before 1.4.2, Common before 2.4.3 and 2.5.x before 2.5.1.

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Annotations</a>	All	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Cache</a>	1.4.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Cache</a>	1.4.1	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Cache</a>	1.4.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Cache</a>	1.4.1	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Cache</a>	All	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Common</a>	2.5.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Common</a>	2.5.0	beta1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Common</a>	2.5.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Common</a>	2.5.0	beta1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Common</a>	All	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Doctrinemongoddbundle</a>	3.0.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Doctrinemongoddbundle</a>	3.0.0	All	All	All

Application	<a href="#">Doctrine-project</a>	<a href="#">Mongodb-odm</a>	All	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	alpha1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	alpha2	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	beta1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	rc1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	rc2	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	All	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	alpha1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	alpha2	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	beta1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	rc1	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	2.5.0	rc2	All	All
Application	<a href="#">Doctrine-project</a>	<a href="#">Object Relational Mapper</a>	All	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.0	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.1	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.2	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.0	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.1	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	2.5.2	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend-cache</a>	All	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend Framework</a>	All	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zend Framework</a>	All	All	All	All
Application	<a href="#">Zend</a>	<a href="#">Zf-apigility-doctrine</a>	All	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-3369-1 zendframework	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
ZF2015-07: Filesystem Permissions Issues in Multiple Components - Advisories - Security - Zend Framework	CONFIRM	<a href="http://framework.zend.com">framework.zend.com</a>
Security Misconfiguration Vulnerability in various Doctrine projects — Doctrine Project	CONFIRM	<a href="http://www.doctrine-project.org">www.doctrine-project.org</a>
[SECURITY] Fedora 24 Update: php-doctrine-common-2.5.3-1.fc24 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 23 Update: php-doctrine-common-2.5.3-1.fc23 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 24 Update: php-doctrine-common-2.5.3-1.fc24 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 23 Update: php-doctrine-common-2.5.3-1.fc23 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

995894 PHP (Composer) Security Update for aws/aws-sdk-php (GHSA-pw5c-xqf2-6xc2)

© [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](#)