



CVE-2015-4050

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

Summary

CVE	CVE-2015-4050
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-02 14:59:00 UTC
Updated	2016-12-31 02:59:00 UTC
Description	FragmentManager in the HttpKernel component in Symfony 2.3.19 through 2.3.28, 2.4.9 through 2.4.10, 2.5.4 through 2.5.1

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sensiolabs	Symfony	2.3.19	All	All	All
Application	Sensiolabs	Symfony	2.3.20	All	All	All
Application	Sensiolabs	Symfony	2.3.21	All	All	All
Application	Sensiolabs	Symfony	2.3.22	All	All	All
Application	Sensiolabs	Symfony	2.3.23	All	All	All
Application	Sensiolabs	Symfony	2.3.24	All	All	All
Application	Sensiolabs	Symfony	2.3.25	All	All	All
Application	Sensiolabs	Symfony	2.3.26	All	All	All
Application	Sensiolabs	Symfony	2.3.27	All	All	All
Application	Sensiolabs	Symfony	2.3.28	All	All	All
Application	Sensiolabs	Symfony	2.4.10	All	All	All
Application	Sensiolabs	Symfony	2.4.9	All	All	All
Application	Sensiolabs	Symfony	2.5.10	All	All	All
Application	Sensiolabs	Symfony	2.5.11	All	All	All
Application	Sensiolabs	Symfony	2.5.4	All	All	All
Application	Sensiolabs	Symfony	2.5.5	All	All	All
Application	Sensiolabs	Symfony	2.5.6	All	All	All

Application	Sensiolabs	Symfony	2.5.7	All	All	All
Application	Sensiolabs	Symfony	2.5.8	All	All	All
Application	Sensiolabs	Symfony	2.5.9	All	All	All
Application	Sensiolabs	Symfony	2.6.0	All	All	All
Application	Sensiolabs	Symfony	2.6.1	All	All	All
Application	Sensiolabs	Symfony	2.6.3	All	All	All
Application	Sensiolabs	Symfony	2.6.4	All	All	All
Application	Sensiolabs	Symfony	2.6.5	All	All	All
Application	Sensiolabs	Symfony	2.6.6	All	All	All
Application	Sensiolabs	Symfony	2.6.7	All	All	All
Application	Sensiolabs	Symfony	2.3.19	All	All	All
Application	Sensiolabs	Symfony	2.3.20	All	All	All
Application	Sensiolabs	Symfony	2.3.21	All	All	All
Application	Sensiolabs	Symfony	2.3.22	All	All	All
Application	Sensiolabs	Symfony	2.3.23	All	All	All
Application	Sensiolabs	Symfony	2.3.24	All	All	All
Application	Sensiolabs	Symfony	2.3.25	All	All	All
Application	Sensiolabs	Symfony	2.3.26	All	All	All
Application	Sensiolabs	Symfony	2.3.27	All	All	All
Application	Sensiolabs	Symfony	2.3.28	All	All	All
Application	Sensiolabs	Symfony	2.4.10	All	All	All
Application	Sensiolabs	Symfony	2.4.9	All	All	All
Application	Sensiolabs	Symfony	2.5.10	All	All	All
Application	Sensiolabs	Symfony	2.5.11	All	All	All
Application	Sensiolabs	Symfony	2.5.4	All	All	All
Application	Sensiolabs	Symfony	2.5.5	All	All	All
Application	Sensiolabs	Symfony	2.5.6	All	All	All
Application	Sensiolabs	Symfony	2.5.7	All	All	All
Application	Sensiolabs	Symfony	2.5.8	All	All	All
Application	Sensiolabs	Symfony	2.5.9	All	All	All
Application	Sensiolabs	Symfony	2.6.0	All	All	All
Application	Sensiolabs	Symfony	2.6.1	All	All	All
Application	Sensiolabs	Symfony	2.6.3	All	All	All
Application	Sensiolabs	Symfony	2.6.4	All	All	All
Application	Sensiolabs	Symfony	2.6.5	All	All	All

Application	Sensiolabs	Symfony	2.6.6	All	All	All
Application	Sensiolabs	Symfony	2.6.7	All	All	All
References						
Reference	Source		Link		Tags	
Debian -- Security Information -- DSA-3276-1 symfony	DEBIAN		www.debian.org			
[SECURITY] Fedora 21 Update: php-symfony-2.5.12-1.fc21	FEDORA		lists.fedoraproject.org			
Symfony CVE-2015-4050 Unauthorized Access Vulnerability	BID		www.securityfocus.com			
[SECURITY] Fedora 22 Update: php-symfony-2.5.12-1.fc22	FEDORA		lists.fedoraproject.org			
CVE-2015-4050: ESI unauthorized access (Symfony Blog)	CONFIRM		symfony.com		Vendor Advisory	
[SECURITY] Fedora 20 Update: php-symfony-2.5.12-1.fc20	FEDORA		lists.fedoraproject.org			
CVE Program record	CVE.ORG		www.cve.org		canonical	
NVD vulnerability detail	NVD		nvd.nist.gov		canonical, analysis	
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