



CVE-2012-2667

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

Summary

CVE	CVE-2012-2667
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-07 19:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Session fixation vulnerability in lib/user/sfBasicSecurityUser.class.php in SensioLabs Symfony before 1.4.18 allows remote

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sensiolabs	Symfony	1.4.0	All	All	All
Application	Sensiolabs	Symfony	1.4.0	rc1	All	All
Application	Sensiolabs	Symfony	1.4.0	rc2	All	All
Application	Sensiolabs	Symfony	1.4.1	All	All	All
Application	Sensiolabs	Symfony	1.4.10	All	All	All
Application	Sensiolabs	Symfony	1.4.11	All	All	All
Application	Sensiolabs	Symfony	1.4.12	All	All	All
Application	Sensiolabs	Symfony	1.4.13	All	All	All
Application	Sensiolabs	Symfony	1.4.14	All	All	All
Application	Sensiolabs	Symfony	1.4.15	All	All	All
Application	Sensiolabs	Symfony	1.4.16	All	All	All
Application	Sensiolabs	Symfony	1.4.2	All	All	All
Application	Sensiolabs	Symfony	1.4.3	All	All	All
Application	Sensiolabs	Symfony	1.4.4	All	All	All
Application	Sensiolabs	Symfony	1.4.5	All	All	All
Application	Sensiolabs	Symfony	1.4.6	All	All	All
Application	Sensiolabs	Symfony	1.4.7	All	All	All

Application	Sensiolabs	Symfony	1.4.8	All	All	All
Application	Sensiolabs	Symfony	1.4.9	All	All	All
Application	Sensiolabs	Symfony	1.4.0	All	All	All
Application	Sensiolabs	Symfony	1.4.0	rc1	All	All
Application	Sensiolabs	Symfony	1.4.0	rc2	All	All
Application	Sensiolabs	Symfony	1.4.1	All	All	All
Application	Sensiolabs	Symfony	1.4.10	All	All	All
Application	Sensiolabs	Symfony	1.4.11	All	All	All
Application	Sensiolabs	Symfony	1.4.12	All	All	All
Application	Sensiolabs	Symfony	1.4.13	All	All	All
Application	Sensiolabs	Symfony	1.4.14	All	All	All
Application	Sensiolabs	Symfony	1.4.15	All	All	All
Application	Sensiolabs	Symfony	1.4.16	All	All	All
Application	Sensiolabs	Symfony	1.4.2	All	All	All
Application	Sensiolabs	Symfony	1.4.3	All	All	All
Application	Sensiolabs	Symfony	1.4.4	All	All	All
Application	Sensiolabs	Symfony	1.4.5	All	All	All
Application	Sensiolabs	Symfony	1.4.6	All	All	All
Application	Sensiolabs	Symfony	1.4.7	All	All	All
Application	Sensiolabs	Symfony	1.4.8	All	All	All
Application	Sensiolabs	Symfony	1.4.9	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All

References						
Reference						Source
IBM X-Force Exchange						XF
oss-security - Re: CVE Request -- Symfony / php-symfony-symfony: Session fixation flaw corrected in upstream 1.4.18 version						MLIST
Security Release: symfony 1.4.18 released - Symfony						CONFIRM
oss-security - CVE Request -- Symfony / php-symfony-symfony: Session fixation flaw corrected in upstream 1.4.18 version						MLIST
Symfony 'regenerate()' Method Session Fixation Vulnerability						BID
/tags/RELEASE_1_4_18/CHANGELOG - symfony - Trac						CONFIRM
About Secunia Research Flexera						SECUNIA
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](#)