

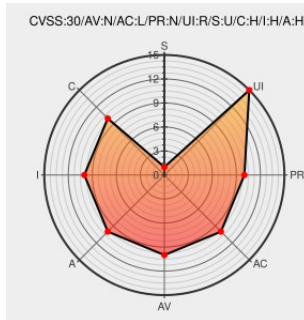


CVE-2018-11406

Published on: 06/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11406

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An issue was discovered in the Security component in Symfony 2.7.x before 2.7.48, 2.8.x before 2.8.41, 3.3.x before 3.3.17, 3.4.x before 3.4.11, and 4.0.x before 4.0.11. By default, a user's session is invalidated when the user is logged out. This behavior can be disabled through the `invalidate_session` option. In this case, CSRF tokens were not erased during logout which allowed for CSRF token fixation.

CVE-2018-11406 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

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
CVE-2018-11406: CSRF Token Fixation (Symfony Blog)	Vendor Advisory symfony.com	CONFIRM symfony.com/blog/cve-2018-11406-csrf-token-fixation

	text/html	
[SECURITY] Fedora 28 Update: php-symfony3-3.4.11-1.fc28 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2018-ba0b683c10
Debian -- Security Information -- DSA-4262-1 symfony	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4262
[SECURITY] Fedora 28 Update: php-symfony4-4.0.11-1.fc28 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2018-96d770ddc9
[SECURITY] Fedora 28 Update: php-symfony-2.8.41-1.fc28 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2018-eba0006df2

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:						
cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)