



CVE-2018-14773

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

Summary

CVE	CVE-2018-14773
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-03 17:29:00 UTC
Updated	2021-09-29 16:21:00 UTC
Description	An issue was discovered in Http Foundation in Symfony 2.7.0 through 2.7.48, 2.8.0 through 2.8.43, 3.3.0 through 3.3.17, 3.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All

References

Reference

[SECURITY] [DLA 1707-1] symfony security update

CVE-2018-14773: Remove support for legacy and risky HTTP headers (Symfony Blog)

Symfony CVE-2018-14773 Security Bypass Vulnerability

[HttpFoundation] Remove support for legacy and risky HTTP headers · symfony/symfony@e447e8b · GitHub

Bugtraq: [SECURITY] [DSA 4441-1] symfony security update

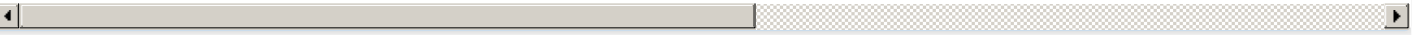
Debian -- Security Information -- DSA-4441-1 symfony

Drupal Access Control Flaw in Symfony HttpFoundation Component Lets Remote Users Bypass Security Restrictions on the Target System -

Drupal Core - 3rd-party libraries -SA-CORE-2018-005 | Drupal.org

CVE Program record

NVD vulnerability detail



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](#)