



CVE-2020-5275

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-5275
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-30 20:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	In symfony/security-http before versions 4.4.7 and 5.0.7, when a `Firewall` checks access control rule, it iterate overs each

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sensiolabs	Symfony	All	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All

References

Reference

All rules set in "access_control" are required when the firewall is configured with the unanimous strategy · Advisory · symfony/symfony · GitHub

[SECURITY] Fedora 32 Update: php-symfony4-4.4.7-1.fc32 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 32 Update: php-symfony4-4.4.7-1.fc32 - package-announce - Fedora Mailing-Lists

security #cve-2020-5275 [Security] Fix access_control behavior with u... · symfony/symfony@c935e4a · GitHub

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](#)