CVE-2020-5275

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

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 · GitHul
[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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report