



CVE-2021-32693

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

Summary

CVE	CVE-2021-32693
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-17 23:15:00 UTC
Updated	2021-06-24 19:00:00 UTC
Description	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. A vulnerability relat

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
CVE-2021-32693: Authentication granted to all firewalls instead of just one (Symfony Blog)	MISC	symfony.co
Authentication granted to all firewalls instead of just one · Advisory · symfony/symfony · GitHub	CONFIRM	github.com
Only trigger for the correct firewall in ContextListener::onKernelRes... · symfony/symfony@3084764 · GitHub	MISC	github.com
security #cve-2021-32693 [SecurityHttp] Fix "Authentication granted w... · symfony/security-http@6bf4c31 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)