



CVE-2023-46734

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

Summary

CVE	CVE-2023-46734
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-10 18:15:00 UTC
Updated	2023-11-16 23:39:00 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Potential XSS vulnerabilities in CodeExtension filters · Advisory · symfony/symfony · GitHub		github.com
security #cve-2023-46734 [TwigBridge] Ensure CodeExtension's filters ... · symfony/symfony@5d095d5 · GitHub		github.com
[TwigBridge] Ensure CodeExtension's filters properly escape their input · symfony/symfony@9da9a14 · GitHub		github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[6000343](#) Debian Security Update for symfony (DLA 3664-1)

[995911](#) PHP (Composer) Security Update for symfony/symfony (GHSA-q847-2q57-wmr3)

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