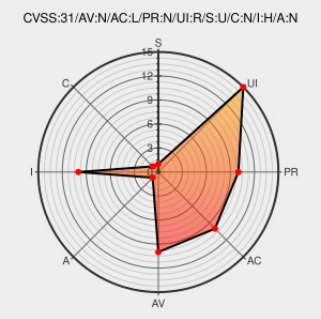
CVE-2021-41267

Published on: 11/24/2021 12:00:00 AM UTC

Last Modified on: 11/30/2021 06:52:00 PM UTC

CVE-2021-41267 - advisory for GHSA-q3j3-w37x-hq2q

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Symfony from Sensiolabs contain the following vulnerability:

Symfony/Http-Kernel is the HTTP kernel component for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Headers that are not part of the "trusted_headers" allowed list are ignored and protect users from "Cache poisoning" attacks. In Symfony 5.2, maintainers added support for the `X-Forwarded-Prefix` headers, but this header was accessible in SubRequest, even if it was not part of the "trusted_headers" allowed list. An attacker could leverage this opportunity to forge requests containing a `X-Forwarded-Prefix` header, leading to a web cache poisoning issue. Versions 5.3.12 and later have a patch to ensure that the `X-Forwarded-Prefix` header is not forwarded to subrequests when it is not trusted.

CVE-2021-41267 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **symfony** - **symfony** version **>= 5.2.0, < 5.3.12**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Webcache Poisoning via X-Forwarded-Prefix and sub-request · Advisory · symfony/symfony · GitHub	github.com text/html	CONFIRM github.com/symfony/symfony/security/advisories/GHSA-q3j3-w37x-hq2q
Fix missing extra trusted header in sub-request · symfony/symfony@95dcf51 · GitHub	github.com text/html	MISC github.com/symfony/symfony/commit/95dcf51682029e89450aee86267e3d553aa7c487
Release v5.3.12 · symfony/symfony · GitHub	github.com text/html	MISC github.com/symfony/symfony/releases/tag/v5.3.12
Release v5.3.12 by fabpot · Pull Request #44243 · symfony/symfony · GitHub	github.com text/html	MISC github.com/symfony/symfony/pull/44243

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@symfony	CVE-2021-41267: Webcache Poisoning via X-Forwarded-Prefix and sub-request symfony.com/blog/cve-2021-… #symfony	2021-11-24 09:13:12
@websagiles	CVE-2021-41267: Webcache Poisoning via X-Forwarded-Prefix and sub-request dlvr.it/SD5tBn https://t.co/ph3IkcHDMn	2021-11-24 11:13:43
@CVEreport	CVE-2021-41267 : Symfony/Http-Kernel is the HTTP #kernel component for Symfony, a PHP framework for web and console… twitter.com/i/web/status/1…	2021-11-24 19:07:24
/r/symfony	CVE-2021-41267: Webcache Poisoning via X-Forwarded-Prefix and sub-request	2021-11-24 10:00:10

← Previous ID

Next ID→

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