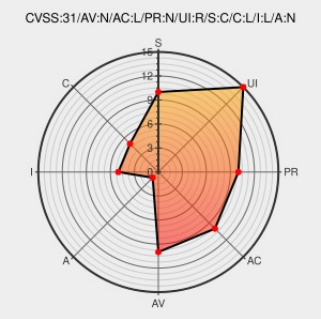
# CVE-2023-32325

Published on: Not Yet Published

Last Modified on: 06/03/2023 03:54:00 AM UTC

## CVE-2023-32325 - advisory for GHSA-8775-5hwv-wr6v

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Posthog-js from Posthog contain the following vulnerability:

PostHog-js is a library to interface with the PostHog analytics tool. Versions prior to 1.57.2 have the potential for cross-site scripting. Problem has been patched in 1.57.2. Users are advised to upgrade. Users unable to upgrade should ensure that their Content Security Policy is in place.

CVE-2023-32325 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **PostHog** - **posthog-js** version **= < 1.57.2**

## CVSS3 Score: 6.1 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | LOW | LOW | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| fix: Remove API and JS urls (#630) · PostHog/posthog-js@67e07eb · GitHub | github.com text/html | MISC github.com/PostHog/posthog-js/commit/67e07eb8bb271a3a6f4aa251382e4d25abb385a0 |
| Potential for cross-site scripting in posthog-js · Advisory · PostHog/posthog-js · GitHub | github.com text/html | MISC github.com/PostHog/posthog-js/security/advisories/GHSA-8775-5hwv-wr6v |

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Posthog | Posthog-js | All | All | All | All |

cpe:2.3:a:posthog:posthog-js:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→