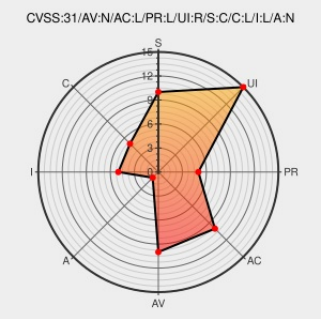
CVE-2023-25571

Published on: Not Yet Published

Last Modified on: 02/23/2023 06:39:00 PM UTC

CVE-2023-25571 - advisory for GHSA-7hv8-3fr9-j2hv

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



Certain versions of Backstage Catalog-model from Linuxfoundation contain the following vulnerability:

Backstage is an open platform for building developer portals. `@backstage/catalog-model` prior to version 1.2.0, `@backstage/core-components` prior to 0.12.4, and `@backstage/plugin-catalog-backend` prior to 1.7.2 are affected by a cross-site scripting vulnerability. This vulnerability allows a malicious actor with access to add or modify content in an instance of the Backstage software catalog to inject script URLs in the entities stored in the catalog. If users of the catalog then click on said URLs, that can lead to an XSS attack. This vulnerability has been patched in both the frontend and backend implementations. The default `Link` component from `@backstage/core-components` version 1.2.0 and greater will now reject `javascript:` URLs, and there is a global override of `window.open` to do the same. In addition, the catalog model v0.12.4 and greater as well as the catalog backend v1.7.2 and greater now has additional validation built in that prevents `javascript:` URLs in known annotations. As a workaround, the general practice of limiting access to modifying catalog content and requiring code reviews greatly help mitigate this vulnerability.

CVE-2023-25571 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **backstage** - **backstage** version **= < 1.2.0**

Affected Vendor/Software: **backstage** - **backstage** version **= < 0.12.4**

Affected Vendor/Software: **backstage** - **backstage** version **= < 1.7.2**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality**	**Integrity**	**Availability**

	Impact	Impact	Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
XSS Vulnerability in Software Catalog · Advisory · backstage/backstage · GitHub	github.com text/html	MISC github.com/backstage/backstage/security/advisories/GHSA-7hv8-3fr9-j2hv
Merge pull request from GHSA-7hv8-3fr9-j2hv · backstage/backstage@3d13719 · GitHub	github.com text/html	MISC github.com/backstage/backstage/commit/3d1371954512f7fa8bd0e2d357e00eada2c3e8a8

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Backstage Catalog-model	All	All	All	All
Application	Linuxfoundation	Backstage Core-components	All	All	All	All
Application	Linuxfoundation	Backstage Plugin-catalog-backend	All	All	All	All

cpe:2.3:a:linuxfoundation:backstage_catalog-model:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:linuxfoundation:backstage_core-components:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:linuxfoundation:backstage_plugin-catalog-backend:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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