



# CVE-2022-32289

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

## Summary

<b>CVE</b>	CVE-2022-32289
<b>State</b>	PUBLIC
<b>Assigner</b>	audit@patchstack.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-21 16:15:00 UTC
<b>Updated</b>	2022-07-25 03:31:00 UTC
<b>Description</b>	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.0 at WordPress leading to popup

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sygnoos</a>	<a href="#">Popup Builder</a>	All	All	All	All

## References

### Reference

- [Popup Builder – Create highly converting, mobile friendly marketing popups. – WordPress plugin | WordPress.org](#)
- [WordPress Popup Builder plugin <= 4.1.0 - Cross-Site Request Forgery \(CSRF\) vulnerability leading to Popup Status Change - Patchstack](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Vulnerability discovered by BEE-K (Patchstack)

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)