



# CVE-2022-33960

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-33960
<b>State</b>	PUBLIC
<b>Assigner</b>	audit@patchstack.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-22 17:15:00 UTC
<b>Updated</b>	2022-07-26 15:19:00 UTC
<b>Description</b>	Multiple Authenticated (subscriber or higher user role) SQL Injection (SQLi) vulnerabilities in Social Share Buttons by Supsys

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Supsysytic	Social Share Buttons	All	All	All	All

## References

Reference	Sou
Social Share Buttons by Supsysytic – WordPress plugin   WordPress.org	COM
WordPress Social Share Buttons by Supsysytic plugin <= 2.2.3 - Multiple Authenticated SQL Injection (SQLi) vulnerabilities - Patchstack	COM
CVE Program record	CVE
NVD vulnerability detail	NVD

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Vulnerability discovered by m0ze (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)