



# CVE-2023-22732

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

## Summary

<b>CVE</b>	CVE-2023-22732
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-17 22:15:00 UTC
<b>Updated</b>	2023-11-07 04:07:00 UTC
<b>Description</b>	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The Administration session expires after 30 minutes of inactivity. This vulnerability allows an attacker to bypass the session expiration and maintain access to the administration interface indefinitely.

## Risk And Classification

**Problem Types:** CWE-613

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shopware	Shopware	All	All	All	All

## References

Reference	Source	Link	Tags
NEXT-24677 - Limit admin session time · shopware/platform@cd7a89c · GitHub	MISC	<a href="https://github.com">github.com</a>	
Shopware 6 - Security Updates - Security Update 01/2023	MISC	<a href="https://docs.shopware.com">docs.shopware.com</a>	
Insufficient Session Expiration in Administration · Advisory · shopware/platform · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analyzed

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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)