



CVE-2021-32711

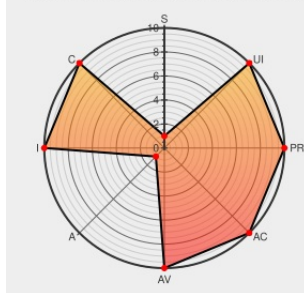
Published on: 06/24/2021 12:00:00 AM UTC

Last Modified on: 07/01/2021 07:55:00 PM UTC

CVE-2021-32711 - advisory for GHSA-f2vv-h5x4-57gr

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Shopware](#) from [Shopware](#) contain the following vulnerability:

Shopware is an open source eCommerce platform. Versions prior to 6.3.5.1 may leak of information via Store-API. The vulnerability could only be fixed by changing the API system, which involves a non-backward-compatible change. Only consumers of the Store-API should be affected by this change. We recommend to update to the current

version 6.3.5.1. You can get the update to 6.3.5.1 regularly via the Auto-Updater or directly via the download overview. <https://www.shopware.com/en/download/#shopware-6> The vulnerability could only be fixed by changing the API system, which involves a non-backward-compatible change. Only consumers of the Store-API should be affected by this change. Please check your plugins if you have it in use. Detailed technical information can be found in the upgrade information. <https://github.com/shopware/platform/blob/v6.3.5.1/UPGRADE-6.3.md#6351> ### Workarounds For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.

<https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659> ### For more information <https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-02-2021>

CVE-2021-32711 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [shopware](#) - platform version < 6.3.5.1

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

Security Update 02/2021

docs.shopware.com
text/html

MISC docs.shopware.com/en/shopware-6-en/security-updates/security-update-02-2021

Leak of information via Store-API · Advisory · shopware/platform · GitHub

github.com
text/html

CONFIRM github.com/shopware/platform/security/advisories/GHSA-f2vv-h5x4-57gr

NEXT-13371 - Fix set flags for api protection flag · shopware/platform@157fb84 · GitHub

github.com
text/html

MISC github.com/shopware/platform/commit/157fb84a8b3b4ace4be165a033d559826704829b

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	Shopware	Shopware	All	All	All	All

cpe:2.3:a:shopware:shopware:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32711 : Shopware is an open source eCommerce platform. Versions prior to 6.3.5.1 may leak of information v... twitter.com/i/web/status/1...	2021-06-24 20:10:49
 /r/netcve	CVE-2021-32711	2021-06-24 20:41:54

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)