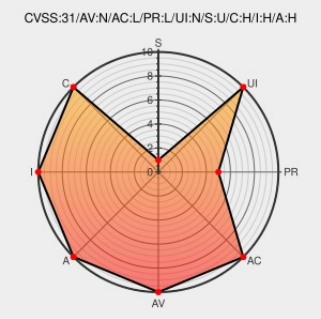
CVE-2021-37711

Published on: 08/16/2021 12:00:00 AM UTC

Last Modified on: 08/24/2021 03:15:00 PM UTC

CVE-2021-37711 - advisory for GHSA-gcvv-gq92-x94r

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



Certain versions of Shopware from Shopware contain the following vulnerability:

Versions prior to 6.4.3.1 contain an authenticated server-side request forgery vulnerability in file upload via URL. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.

CVE-2021-37711 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **shopware** - **platform** version **<= 6.4.3.0**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Authenticated server-side request forgery in file upload via URL. · Advisory · shopware/platform ·	github.com text/html	CONFIRM github.com/shopware/platform/security/advisories/GHSA-gcvv-gq92-x94r

GitHub

NEXT-15673 - Fix file upload ip validation for IPv6 · shopware/platform@b9f330e · GitHub	github.com text/html	MISC github.com/shopware/platform/commit/b9f330e652b743dd2374c02bbe68f28b59a3f502

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-2021-37711 : Versions prior to 6.4.3.1 contain an authenticated server-side request forgery vulnerability in fi… twitter.com/i/web/status/1…	2021-08-16 22:27:00

← Previous ID

Next ID→