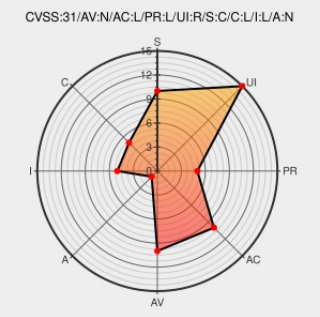
CVE-2022-23065

Published on: Not Yet Published

Last Modified on: 05/10/2022 04:34:00 PM UTC

CVE-2022-23065 - advisory for https://www.whitesourcesoftware.com/vulnerability-database/

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



Certain versions of Vendure from Vendure contain the following vulnerability:

In Vendure versions 0.1.0-alpha.2 to 1.5.1 are affected by Stored XSS vulnerability, where an attacker having catalog permission can upload a SVG file that contains malicious JavaScript into the “Assets” tab. The uploaded file will affect administrators as well as regular users.

CVE-2022-23065 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **vendure-ecommerce** - **vendure** version **>= 0.1.0-alpha.2**

Affected Vendor/Software: **vendure-ecommerce** - **vendure** version **<= 1.5.1**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2022-23065 | WhiteSource Vulnerability Database	www.whitesourcesoftware.com text/html	MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2022-23065
fix(asset-server-plugin): Fix svg XSS vulnerability · vendure-ecommerce/vendure@69a4486 · GitHub	github.com text/html	MISC github.com/vendure-ecommerce/vendure/commit/69a44869112c0a5b836e2ddd3969ea9b533f51

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vendure	Vendure	0.1.0	alpha10	All	All
Application	Vendure	Vendure	0.1.0	alpha11	All	All
Application	Vendure	Vendure	0.1.0	alpha12	All	All
Application	Vendure	Vendure	0.1.0	alpha13	All	All
Application	Vendure	Vendure	0.1.0	alpha14	All	All
Application	Vendure	Vendure	0.1.0	alpha15	All	All
Application	Vendure	Vendure	0.1.0	alpha16	All	All
Application	Vendure	Vendure	0.1.0	alpha18	All	All
Application	Vendure	Vendure	0.1.0	alpha2	All	All
Application	Vendure	Vendure	0.1.0	alpha3	All	All
Application	Vendure	Vendure	0.1.0	alpha4	All	All
Application	Vendure	Vendure	0.1.0	alpha5	All	All
Application	Vendure	Vendure	0.1.0	alpha6	All	All
Application	Vendure	Vendure	0.1.0	alpha7	All	All
Application	Vendure	Vendure	0.1.0	alpha8	All	All
Application	Vendure	Vendure	0.1.0	alpha9	All	All
Application	Vendure	Vendure	All	All	All	All

cpe:2.3:a:vendure:vendure:0.1.0:alpha10:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha11:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha12:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha13:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha14:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha15:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha16:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha18:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha3:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha4:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha5:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha6:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha7:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha8:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:0.1.0:alpha9:*:*:*:*:*:*:

cpe:2.3:a:vendure:vendure:*:*:*:*:*:*:*:*:

Discovery Credit

WhiteSource Vulnerability Research Team (WVR)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23065 : In Vendure versions 0.1.0-alpha.2 to 1.5.1 are affected by Stored #XSS vulnerability, where an att… twitter.com/i/web/status/1…	2022-05-02 12:35:15
/r/netcve	CVE-2022-23065	2022-05-02 13:40:31

← Previous ID

Next ID→