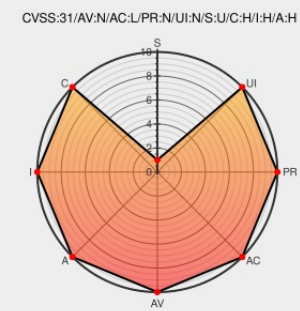
CVE-2022-40305

Published on: Not Yet Published

Last Modified on: 09/10/2022 03:53:00 AM UTC

CVE-2022-40305

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



Certain versions of Canto from Canto contain the following vulnerability:

A Server-Side Request Forgery issue in Canto Cumulus through 11.1.3 allows attackers to enumerate the internal network, overload network resources, and possibly have unspecified other impact via the server parameter to the /cwc/login login form.

CVE-2022-40305 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
	www.syss.de text/plain	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-023.txt

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	Canto	Canto	All	All	All	All

cpe:2.3:a:canto:canto:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-40305 : A Server-Side Request Forgery issue in Canto Cumulus through 11.1.3 allows attackers to enumerate… twitter.com/i/web/status/1…	2022-09-09 05:04:59
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-40305 A Server-Side Request Forgery issue in Canto Cumulus through 11.1… twitter.com/i/web/status/1…	2022-09-09 06:56:00
/r/netcve	CVE-2022-40305	2022-09-09 06:38:33

← 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 registred 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