Data Space Portal: Incorrect Authorization and Client-Side Enforcement of Server-Side Security in ghcr.io/sovity/ds-portal-ce-backend

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-42160
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 20:16:30 UTC
Updated	2026-05-11 19:16:23 UTC
Description	Data Space Portal is an open-source Software as a Service (SaaS) solution designed to streamline Dataspace managemer

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000720000 probability, percentile 0.216860000 (date 2026-05-12)

Problem Types: CWE-602 | CWE-863 | CWE-602 CWE-602: Client-Side Enforcement of Server-Side Security | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/
4.0	CNA	DECLARED	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sovity	Dataspace-portal	affected >= 2.1.1, < 7.3.2	Not specified

References

Reference	Source	Link	T
github.com/sovity/dataspace-portal/security/advisories/GHSA-989g-wpfv-6vxx	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
github.com/sovity/dataspace-portal/releases/tag/v7.3.2	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report