



# Chartbrew Cross-Tenant Template Export and Secret Disclosure in `GET /team/:team\_id/template/generate/:project\_id`

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-32252
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-10 20:16:21 UTC
<b>Updated</b>	2026-04-14 17:25:25 UTC
<b>Description</b>	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create of

## Risk And Classification

**Primary CVSS:** v3.1 7.7 HIGH from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**EPSS:** 0.000260000 probability, percentile 0.070750000 (date 2026-04-15)

**Problem Types:** CWE-285 | CWE-285 CWE-285: Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	DECLARED	7.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Depomo	Chartbrew	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Chartbrew	Chartbrew	affected < 4.9.0	Not specified

### References

Reference	Source	Link
github.com/chartbrew/chartbrew/commit/bf5919043d3587fcbe76123aaabd9a0a9d...	security-advisories@github.com	github.com
github.com/chartbrew/chartbrew/security/advisories/GHSA-mw4f-cf22-qpcj	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)