



# Sensitive Data Disclosure in BigQuery via Materialized View Error Messages

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

## Summary

<b>CVE</b>	CVE-2026-3259
<b>State</b>	PUBLISHED
<b>Assigner</b>	GoogleCloud
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-23 10:16:16 UTC
<b>Updated</b>	2026-04-23 10:16:16 UTC
<b>Description</b>	A Generation of Error Message Containing Sensitive Information vulnerability in the Materialized View Refresh mechanism

## Risk And Classification

**Primary CVSS:** v4.0 7.1 HIGH from f45cbf4e-4146-4068-b7e1-655ffc2c548c

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

**Problem Types:** CWE-209 | CWE-209 CWE-209 Generation of error message containing sensitive information

Version	Source	Type	Score	Severity	Vector
4.0	f45cbf4e-4146-4068-b7e1-655ffc2c548c	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Cloud	BigQuery	affected 01/29/2026 date	Not specified

### References

Reference	Source	Link	Tags
docs.cloud.google.com/bigquery/docs/release-notes	f45cbf4e-4146-4068-b7e1-655ffc2c548c	docs.cloud.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Gonzalo López Zuloaga (en)

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)