



Corteza 2024.9.8 - SQL Injection in MSSQL JSON-path meta filter via incorrect T-SQL string escaping

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

Summary

CVE	CVE-2026-6093
State	PUBLISHED
Assigner	Fluid Attacks
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 16:17:36 UTC
Updated	2026-05-12 18:56:44 UTC
Description	Corteza contains a SQL injection vulnerability in its Microsoft SQL Server (MSSQL) backend when filtering Compose records

Risk And Classification

Primary CVSS: v4.0 6 MEDIUM from help@fluidattacks.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/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:X

EPSS: 0.000300000 probability, percentile 0.087190000 (date 2026-05-12)

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
4.0	help@fluidattacks.com	Secondary	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/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:X
4.0	CNA	CVSS	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/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:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cortezaproject	Corteza	affected 2024.9.8	Windows, MacOS, Linux

References

Reference	Source	Link	Tags
github.com/cortezaproject/corteza	help@fluidattacks.com	github.com	
fluidattacks.com/es/advisories/motley	134c704f-9b21-4f2e-91b3-4a467353bcc0	fluidattacks.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: Fluid Attacks' AI SAST Scanner (en)

CNA: Oscar Uribe (en)

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

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

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