SurrealDB injection via unsanitized order_by parameter

High **lfnovo** published **GHSA-5wj9-f8q5-8f9c** last month

Package

open-notebook

Affected versions

<= 1.8.2

Patched versions

1.8.3

Description

The `GET /api/notebooks` endpoint accepted arbitrary user input in the `order_by` query parameter, which was interpolated directly into a SurrealQL query without validation or sanitization. This allowed injection of arbitrary database commands.

Since the injection was in a GET request, it was exploitable via cross-site request forgery (CSRF) by tricking a user into clicking a crafted URL. An attacker could create, modify, or delete arbitrary database records. Data exfiltration was also possible with the default CORS configuration.

Impact

- Alter or delete arbitrary database entries (notebooks, sources, notes, chat sessions)
- Data exfiltration possible with default CORS configuration

Patches

Fixed in v1.8.3. Upgrade immediately.

Credit

Reported by CERT-EU Offensive Security Team.

Severity

High 8.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

▶ CWE-89