

[payloadcms](#) / [payload](#) Public[Code](#) [Issues](#) 282 [Pull requests](#) 494 [Discussions](#) [Actions](#) [Projects](#)

# SQL Injection via Query Handling

High [denolfe](#) published [GHSA-7xxh-373w-35vg](#) 2 days ago

## Package

 [payload](#) (npm)

### Affected versions

&lt; 3.79.1

### Patched versions

3.79.1

## Description

### Impact

Certain request inputs were not properly validated. An attacker could craft requests that influence SQL query execution, potentially exposing or modifying data in collections.

### Patches

This issue has been fixed in **v3.79.1** and later. Query input validation has been hardened.

Upgrade to **v3.79.1** or later.

### Workarounds

Until you can upgrade:

- Limit access to endpoints that accept dynamic query inputs to trusted users only.
- Validate or sanitize input from untrusted clients before sending it to query endpoints.

## Severity

High 8.5 / 10

### CVSS v3 base metrics

Attack vector

Network

Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	None
<a href="#">Learn more about base metrics</a>	

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

### CVE ID

CVE-2026-34747

### Weaknesses

▶ CWE-89

### Credits



**hessandrew**

Reporter



**arkmarta**

Reporter