Stored XSS in Admin Panel

High **denolfe** published **GHSA-mmxc-95ch-2j7c** last week

Package

@payloadcms/next (npm)

Affected versions

< 3.78.0

Patched versions

3.78.0

Description

Impact

A stored Cross-Site Scripting (XSS) vulnerability existed in the admin panel. An authenticated user with write access to a collection could save content that, when viewed by another user, would execute in their browser.

You are affected if ALL of these are true:

- Payload version **< v3.78.0**
- At least one collection with versions enabled
- An authenticated user has `create` or `update` access to that collection

Patches

This vulnerability has been patched in **v3.78.0**. Output encoding has been added to prevent user-supplied content from being interpreted as markup.

Users should upgrade to **v3.78.0** or later.

Workarounds

If you cannot upgrade immediately:

- Restrict `create` and `update` access to versioned collections to trusted roles only.

Severity

High 8.7 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34748

Weaknesses

▶ CWE-79