COMMUNITY CONTENT

Home › Submit › 780613

Submit #780613: z-9527 admin ≤ commit 72aaf2d Cross Site Scripting

Title	z-9527 admin ≤ commit 72aaf2d Cross Site Scripting
Description	A stored Cross-Site Scripting (XSS) vulnerability exists in Z-9527 Admin ≤ commit 72aaf2d at the message board functionality, where the /message/create endpoint accepts user-supplied message content without sanitization or validation, stores it directly in the database, and the React frontend renders this content using dangerouslySetInnerHTML without sanitization or validation. As a result, authenticated attackers can inject arbitrary JavaScript that executes in the browsers of users viewing the message board, potentially leading to session hijacking, credential theft, or malicious actions performed on behalf of victims. Mitigations include implementing HTML sanitization using libraries like DOMPurify, avoiding dangerouslySetInnerHTML in favor of safe React rendering, implementing Content Security Policy (CSP) headers, encoding output context-appropriately, and validating input against a whitelist of allowed HTML tags and attributes.
Source	⚠ https://github.com/CC-T-454455/Vulnerabilities/tree/master/z9527-admin/vulnerability-10
User	Anonymous User
Submission	03/16/2026 04:45 AM (16 days ago)
Moderation	03/31/2026 06:11 PM (16 days later)
Status	Accepted
VulDB entry	354442 [z-9527 admin 1.0/2.0 Message Create Endpoint message.js cross site scripting]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling