



Home > Submit > 782265

# Submit #782265: 1Panel-dev MaxKB <= v2.6.1 Stored XSS

<b>Title</b>	1Panel-dev MaxKB <= v2.6.1 Stored XSS
<b>Description</b>	A Stored Cross-Site Scripting (XSS) vulnerability exists in MaxKB. Authenticated users with dataset management permissions can create paragraphs containing arbitrary HTML/Markdown content. The application stores this content without sanitization and subsequently renders it in the UI using the md-editor-v3 MdPreview component, which does not sanitize HTML by default. This allows attackers to inject malicious JavaScript that executes when other users, including administrators, view the paragraph or execution details.
<b>Source</b>	<a href="https://github.com/AnalogyC0de/public_exp/issues/28">https://github.com/AnalogyC0de/public_exp/issues/28</a>
<b>User</b>	 Analogy (UID: 93258)
<b>Submission</b>	03/18/2026 01:07 PM (26 days ago)
<b>Moderation</b>	04/11/2026 09:35 AM (24 days later)
<b>Status</b>	<span style="background-color: #28a745; color: white; padding: 2px;">Approved</span>
<b>VulDB entry</b>	<a href="#">VUL-2026-00000</a> [1Panel-dev MaxKB up to 2.4.2 MdPreview ui/src/chat.ts cross site scripting]
<b>Points</b>	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](#)