Stored XSS via Unsanitized html_rander Tags in Markdown Rendering

Moderate **liqiang-fit2cloud** published **GHSA-3rq5-pgm7-pvp4** yesterday

Package

MaxKB

Affected versions

<=v2.7.1

Patched versions

v2.8.0

Description

Summary

A Stored Cross-Site Scripting (XSS) vulnerability exists in MaxKB when creating or updating Application configurations. The prologue (Opening Remarks) field allows authenticated users to inject arbitrary HTML and JavaScript by wrapping the malicious payload in <html_rander> tags. When any visitor opens the chatbot interface for this application, the frontend renders the raw HTML, allowing the attacker to execute arbitrary JavaScript in the victim's browser. This could lead to session hijacking, unauthorized actions performed on behalf of the victim (such as deleting workspaces or applications), and sensitive data exposure.

Details

MaxKB allows rendering custom HTML elements using the <html_rander> pseudo-tag to support advanced Markdown integration for customized chatbot welcome messages (prologue). The vulnerability stems from an insecure implementation in apps/application/serializers/application.py, specifically within the ApplicationCreateSerializer and SimulationRequest models. When an application is created or updated via the /admin/api/workspace/{workspace_id}/application API endpoint, the backend directly retrieves the prologue field from the submitted JSON payload and saves it into the database without rigorous HTML entity encoding or tag sanitization.

Because the frontend intrinsically trusts content wrapped in <html_rander> to be safe, it leverages an innerHTML-equivalent mechanism to render it. This allows an attacker to easily break out using standard HTML elements like <script>, <iframe> or , leading to persistent DOM-based Stored XSS execution against anyone who visits the application's chat UI.

Severity

Moderate

CVE ID

CVE-2026-39425

Weaknesses

No CWEs