Stored XSS via Unsanitized iframe_render Parsing in MaxKB

Moderate **liqiang-fit2cloud** published **GHSA-q2qg-43vq-f2wv** yesterday

Package

MaxKB

Affected versions

<=v2.7.1

Patched versions

v2.8.0

Description

Summary
A critical Stored Cross-Site Scripting (XSS) vulnerability exists in MaxKB. The frontend application parses custom <iframe_render> tags from LLM responses or Application Prologue configurations, bypassing standard Markdown sanitization. The extracted content is then rendered directly into an <iframe> configured with sandbox="allow-scripts allow-same-origin", enabling arbitrary JavaScript execution in the context of the parent window.

Details
The MdRenderer.vue component in MaxKB intercepts custom tags like <iframe_render> prior to standard XSS filtering by plugins like XSSPlugin. This untreated content is delegated to the IframeRender.vue component, which assigns the unsanitized HTML directly to the srcdoc attribute of an <iframe>.

Crucially, this iframe uses sandbox="allow-scripts allow-same-origin". This dangerous combination of permissions allows any injected script to break out of the iframe and execute JavaScript in the parent window using window.parent. Since the Prologue is rendered for any user visiting an application's chat interface, this results in a high-impact Stored XSS that bypasses the built-in regex filters (which natively leave script_exec = True).

Severity

Moderate

CVE ID

CVE-2026-39426

Weaknesses

No CWEs