

# [HCSEC-2026-01 - Arbitrary code execution in React server-side rendering of untrusted MDX content](#)

---

[dduzgun-security](#) 1 February 12, 2026, 1:26am

**Bulletin ID:** HCSEC-2026-01

**Affected Products / Versions:** next-mdx-remote from 4.3.0 up to 5.0.0, fixed in 6.0.0.

**Publication Date:** February 11, 2026

## Summary

The serialize function used to compile MDX in next-mdx-remote is vulnerable to arbitrary code execution due to insufficient sanitization of MDX content. This vulnerability, CVE-2026-0969, is fixed in next-mdx-remote 6.0.0.

## Background

[next-mdx-remote](#) is an open-source TypeScript library that allows MDX content from various sources to be rendered dynamically on the client or server.

## Details

Allowing untrusted user MDX content with JavaScript expressions enabled may lead to remote code execution (RCE) due to improper sanitization. As of version 6.0.0, next-mdx-remote introduces a breaking change that disables JavaScript expressions by default ( `enableJsExpressions: false` ) for both `serialize` and `render` functions. When JavaScript expressions are enabled ( `enableJsExpressions: true` ), the new `enableDangerousOperations` option (enabled by default) provides best-effort protection against dangerous operations like `eval`, `execScript`, `Function`, `new Function`, and other globals that could lead to arbitrary code execution.

## Remediation

Deployments allowing untrusted user inputs to the `serialize` or `render` function from the next-mdx-remote library in a server environment should evaluate the risk associated with this issue and consider upgrading to next-mdx-remote 6.0.0.

## Acknowledgement

This issue was identified by Gagyeong Kim from Sejong University.

*We deeply appreciate any effort to coordinate disclosure of security vulnerabilities. For information about security at HashiCorp and the reporting of security vulnerabilities, please see*

<https://hashicorp.com/security>.

2 Likes

## Related topics

Topic	Replies	Activity
<a href="#">HCSEC-2020-08 - Nomad's Raw File View Vulnerable to Cross-Site Scripting</a> <a href="#">security-nomad</a>	0	November 25, 2020
<a href="#">HCSEC-2024-24 - Consul Vulnerable To Reflected XSS On Content-Type Error Manipulation</a> <a href="#">security-consul</a>	0	October 30, 2024
<a href="#">HCSEC-2020-21 - Nomad File Sandbox Escape via Template and Artifact Stanzas</a> <a href="#">security-nomad</a>	0	November 25, 2020
<a href="#">HCSEC-2023-17 - Vault's KV Diff Viewer Allowed HTML Injection</a> <a href="#">security-vault</a>	0	June 9, 2023
<a href="#">HCSEC-2026-06 - Vault Vulnerable to Server-Side Request Forgery in ACME Challenge Validation via Attacker-Controlled DNS</a> <a href="#">security-vault</a>	0	April 17, 2026