GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

8 July 2026

Advisory 154: CVE-2026-57756: Contributor SQL Injection in nicen-localize-image Vulnerability.

Release Date: 06th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

A SQL Injection vulnerability affecting the **nicen-localize-image** WordPress plugin, versions 1.4.9 and earlier. This is classified as a "Contributor" level vulnerability — meaning it requires an authenticated user with at least Contributor-role privileges (WordPress's lowest privileged content-creation role) to exploit, rather than being reachable by a fully unauthenticated attacker.

What are the systems affected?

Any WordPress installation running the nicen-localize-image plugin at version 1.4.9 or earlier. This plugin is used for localizing/translating image metadata within WordPress media libraries.

What does this mean?

The vulnerability allows a user with Contributor-level access (a low privilege tier, often granted to guest authors or content submitters) to inject malicious SQL through plugin functionality without proper input sanitization or parameterized queries. Since Contributor is one of the lowest authenticated roles in WordPress, this significantly lowers the bar for exploitation compared to admin-only SQLi flaws — any compromised or malicious low-privilege account (e.g., a guest contributor account, or one obtained via credential stuffing/phishing) could be leveraged to query or manipulate the underlying database, potentially exposing user data, session tokens, or other sensitive database contents depending on the plugin's query context.

Mitigation process

CERTVU recommends the following:

- **Check plugin usage:** Confirm whether any WordPress site in your environment (if WordPress is in use anywhere alongside the Joomla vhosts) has nicen-localize-image installed, and at what version.
- **Update immediately** if a patched version (>1.4.9) has been released — check the WordPress.org plugin repository or the plugin vendor's changelog directly, since this wasn't specified in available advisory data at the time of this search.
- **If no patch is available yet:** Restrict or audit Contributor-level account creation and review existing Contributor accounts for signs of compromise (unexpected login locations, unfamiliar accounts).
- **General hardening regardless of patch status:** Enable a WAF rule set (e.g., Wordfence, Sucuri) that includes signature detection for WordPress plugin SQLi patterns, since these often get virtual-patched quickly by WAF vendors even before an official plugin fix ships.

Reference

1. https://www.cisa.gov/news-events/bulletins/sb26-187
2. https://www.cve.org/CVERecord?id=CVE-2026-57756

.