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

28 August 2026

Advisory 206: CVE-2026-65876_SP Page Builder for Joomla Unauthenticated SQL Injection - Urgent Update to CERTVU Advisory 160

Release Date: 27th August 2026
Impact: CRITICAL
TLP: CLEAR

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

Urgent notice to recipients of CERTVU Advisory 160

CERTVU Advisory 160, issued on 7 July 2026, addressed CVE-2026-48908, an unauthenticated file upload vulnerability in the SP Page Builder extension for Joomla, and directed organisations to upgrade to version 6.6.2.

That guidance is no longer sufficient. A second and distinct vulnerability, CVE-2026-65876, has since been identified in the same extension. Version 6.6.2 closed only the file upload flaw. The entire 6.x series up to and including 6.7.1 remains vulnerable to this second issue, and only version 6.8.0 resolves both.

Organisations that acted correctly on Advisory 160 and upgraded to 6.6.2 are therefore still exposed. CERTVU is issuing this advisory specifically to correct that position, and asks that it be brought to the attention of anyone who acted on the earlier advisory.

What is it?

CVE-2026-65876 is an unauthenticated SQL injection vulnerability in the SP Page Builder extension for Joomla. The flaw is reachable through the extension's load more endpoint and requires no authentication, allowing a remote attacker to read the contents of the site database.

It has been characterised as a critical zero-day and is reported to be under active exploitation. It is distinct from **CVE-2026-48908**, which affected the custom icon upload feature and carried a CVSS 4.0 score of 10.0 and was addressed in CERTVU Advisory 160.

A Joomla site database holds user account records including password hashes, session data, configuration values and the content of the site itself. Read access to it is sufficient to support account compromise and to inform further attacks against the site and its administrators.

What are the systems affected?

SP Page Builder, all 6.x versions up to and including 6.7.1 - (Affected)

SP Page Builder 6.8.0 and later - (Not affected, patched)

Version 6.6.2, previously advised under CERTVU Advisory 160, remains affected by this vulnerability. The extension is one of the most widely installed Joomla extensions, and affects sites running Joomla 3, 4, 5 and 6 alike. A fully updated Joomla core does not provide protection, because the flaw is in the extension rather than in Joomla itself.

To check the installed version, log in to the Joomla administrator, open Extensions, then Manage, then Manage, and filter for SP Page Builder. If the version shown is 6.7.1 or below, the site is vulnerable.

What does this mean?

CERTVU draws particular attention to three points.

First, updating alone does not remove an attacker who is already present. Where a site has been compromised through either this vulnerability or the earlier file upload flaw, the update closes the entry point but leaves any accounts, backdoors or scheduled tasks the attacker created fully intact. Remediation must include a compromise assessment.

Second, disabling or unpublishing the extension is not an effective mitigation. The vulnerable endpoints remain reachable through the component controller regardless of whether any page using the extension is published.

Third, web application firewall rules written for the earlier JCE and SP Page Builder file upload campaigns will not necessarily block this vulnerability, because it is a different flaw reached through a different endpoint. Organisations relying on a firewall rule as an interim control should not assume existing coverage extends to this issue.

CERTVU notes that this vulnerability arises in the same product family that has featured in local intrusion activity. Organisations operating public-facing Joomla sites in Vanuatu should treat this as a priority.

Indicators of Compromise

Published indicators associated with exploitation of SP Page Builder include:

- Hidden or unrecognised Super User accounts, in some cases created with email addresses ending in @secure.local
- PHP backdoor files placed within the web root, including in extension and media directories
- Unexpected requests to SP Page Builder component endpoints in web server access logs, particularly from unfamiliar source addresses
- Unexpected administrator accounts, user group changes, or template and plugin modifications
- Unexplained outbound connections from the web server, or unexpected scheduled tasks

Mitigation process

CERTVU recommends the following:

1. **Upgrade to SP Page Builder 6.8.0 Immediately**

Upgrade to version 6.8.0 or later. Do not treat version 6.6.2 as remediation, notwithstanding the guidance in CERTVU Advisory 160, which this advisory supersedes. Given that the vulnerability is unauthenticated, reachable from the internet and under active exploitation, this should be treated as an emergency change.

2. **Audit All Joomla Sites for the Extension**

Identify every Joomla site in your estate, including sites maintained by an external web developer or hosting provider, and determine whether SP Page Builder is installed and at what version. Ask any external provider directly rather than assuming they have acted.

Other mitigating options include;

- Conduct a Compromise Assessment
- Rotate Credentials and Reset Sessions
- Restrict Administrative Access

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-65876
2. https://www.cve.org/CVERecord?id=CVE-2026-48908
3. https://vel.joomla.org/
4. https://www.joomshaper.com/
5. https://www.cisa.gov/known-exploited-vulnerabilities-catalog