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 160: CVE-2026-48908_SP Page Builder for Joomla_Unauthenticated File Upload RCE

Release Date: 07th 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?

SP Page Builder exposes a controller task, `asset.uploadCustomIcon` (reachable via `index.php?option=com_sppagebuilder&task=asset.uploadCustomIcon`), intended to let an administrator upload a custom icon-font package. In affected versions, this endpoint performs:

- **No authentication or authorization check** — it's reachable by anyone, not just logged-in administrators.
- **No anti-CSRF token validation.**
- **No server-side file-type validation** on the uploaded content.

What are the systems affected?

Any Joomla site running SP Page Builder version 6.6.1 or earlier. Given SP Page Builder's popularity as a Joomla page-builder extension, and that this requires no authentication, any internet-

facing Joomla instance with this extension installed should be treated as exposed regardless of whether the site's public content itself looks unrelated to page-builder functionality.

What does this mean?

How it's exploited:

- Attacker sends an unauthenticated HTTP request to the `asset.uploadCustomIcon` task with a crafted ZIP archive in the `custom_icon` multipart field.
- Because there's no auth check, no CSRF token requirement, and no file-type validation, the server accepts the request and extracts the ZIP's contents into the public `media/com_sppagebuilder/assets/iconfont/<name>/` path.
- If the archive contains a PHP file rather than legitimate icon-font assets, that PHP file now sits in a browsable, web-served directory.
- Attacker requests the uploaded PHP file directly over HTTP. If the web server executes PHP from that upload path (true for common Apache/PHP configurations), the attacker's code runs with the privileges of the web server — full remote code execution, pre-authentication.
- Public proof-of-concept exploit code for this vulnerability is already circulating, which is consistent with the active exploitation CISA/vendors have observed.

Mitigation process

CERTVU recommends the following:

• **Patch immediately:** Update SP Page Builder to 6.6.2 or later via the Joomla Extensions Manager. The fix gates `uploadCustomIcon` behind an authenticated session, requires admin/component-manage permission, and enforces a valid anti-CSRF token.

• **If you can't patch immediately:**

- Disable or uninstall SP Page Builder until the update can be applied.
- Prevent PHP execution from upload/media directories at the web-server level (e.g., deny `.php` execution under `/media/com_sppagebuilder/assets/`) — this doesn't stop the unauthenticated file write but blocks the path to code execution.
- Restrict external access to the Joomla site (or at minimum the vulnerable endpoint) at the network/WAF level while a maintenance window is arranged.
- If running RSFirewall, version 3.3.7 includes a rule that mitigates this specific exploitation path.

Reference

1. https://www.cisa.gov/news-events/alerts/2026/07/07/cisa-adds-three-known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-48908