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 162: CVE-2026-56290 — Joomlack Page Builder Improper Access Control Vulnerability

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?

Page Builder CK's front-end controller method `browse.ajaxAddPicture` accepts a file upload and a destination path with no authentication or authorization check at all. The only control present is a CSRF token — but that token is retrievable by anyone from the extension's own public-facing pages with a single request, so it provides no real protection against an unauthenticated attacker. The handler takes the uploaded file and a user-supplied `path` parameter (only trimmed, not validated) and writes the file to that attacker-chosen, web-accessible location.

What are the systems affected?

Any Joomla site (Joomla 3, 4, 5, or 6) running Page Builder CK 3.5.10 or earlier. Because the vulnerable endpoint is front-end and requires no login**,** any internet-facing Joomla site with this extension installed is exposed, regardless of whether the extension is actively used in visible page content.

What does this mean?

How it's exploited:

• Attacker fetches a valid CSRF token from any public page on the target site — no login needed.
• Attacker sends a request to `index.php?option=com_pagebuilderck&task=browse.ajaxAddPicture` (or related tasks such as `fonts.save`, seen in observed exploit chains), supplying a crafted file and a destination path under the component's writable media directory (e.g., `media/com_pagebuilderck/gfonts/`).
• Because there is no authentication check and no meaningful validation of the file's content or destination, a PHP file is written directly into a web-served folder.
• Attacker requests the uploaded PHP file over HTTP, and it executes with the privileges of the web server — full remote code execution, unauthenticated, in a single request chain.

Mitigation process

CERTVU recommends the following:

Patch immediately, matched to your Joomla version:

- Joomla 5/6: update Page Builder CK to **3.6.0**
- Joomla 4: update to the back-ported **3.4.10**
- Joomla 3: update to the back-ported **3.1.1**

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-2026-56290