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 207: Joomla Core and Extension Security Update_August 2026 Consolidated Advisory

Release Date: 18th August 2026
Impact: HIGH
TLP: CLEAR

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

Any organisation operating a website built on the Joomla content management system, and any organisation whose website is maintained on its behalf by an external web developer or hosting provider. Joomla is widely used across government, business and community websites in Vanuatu.

This advisory consolidates the current Joomla security position as at August 2026. It should be read together with CERTVU Advisory 206, which addresses an urgent and separate issue in the SP Page Builder extension.

What is it?

This advisory covers two matters: the current Joomla core security release, and the substantially larger body of risk arising from third-party extensions.

CERTVU emphasises the second point at the outset. Joomla core is maintained by a dedicated Security Strike Team, is patched promptly, and can be updated in a single step. The extensions installed alongside it are written by many different third-party developers of varying capability, are updated on no common schedule, and are where the overwhelming majority of Joomla site compromises begin. An organisation that keeps its Joomla core current and neglects its extensions is not protected.

Joomla core: current security release

The Joomla Project released Joomla 6.1.3 and Joomla 5.4.8 on 18 August 2026. These are security and bugfix releases addressing seven core issues:

- Response header injection in download views
- Improper CORS origin validation
- Inconsistent access control checks for mutating webservice endpoints
- Improper access control checks for custom fields webservice endpoints
- Improper access control checks for category webservice endpoints
- Cross-site scripting through schema.org outputs
- Multi-factor authentication bypass

The multi-factor authentication bypass is the most significant of the seven. Organisations that have deployed MFA on Joomla administrator accounts as a compensating control should not assume that control is effective until this update is applied.

CERTVU also draws attention to the recurring pattern in these releases. Four of the seven issues concern access control on webservice, or REST API, endpoints. The preceding release addressed similar issues, and CVE-2026-48904 allows privilege escalation through the com_users group editing webservice endpoint. Where the Joomla webservices are not required for the operation of a site, CERTVU recommends they be disabled.

Joomla 5.4.x continues to receive security patches until October 2027, so organisations whose extensions are not yet compatible with the Joomla 6 series may update to 5.4.8 rather than migrating immediately.

Joomla extensions: the principal area of risk

Between mid-June and late July 2026, security researchers publicly disclosed nineteen separate vulnerabilities across seventeen widely used Joomla extensions. Most were rated critical, five carried the maximum CVSS 4.0 score of 10.0, and several were reported to be exploited in the wild within hours of the fix being made public. Disclosures continued through August.

Three extension vulnerabilities warrant specific attention:

Joomla Content Editor (JCE), CVE-2026-48907. An improper access control flaw in the profile import functionality allows an unauthenticated attacker to create a malicious editor profile and upload executable PHP content to the server.

Administrators should note that the version guidance has moved: version 2.9.99.5 addressed the original flaw, 2.9.99.6 added hardening, and 2.9.99.7 provided further hardening and fixed upload-related issues found after 2.9.99.6. Organisations should update to 2.9.99.7 or later, not merely to 2.9.99.5.

Extensions with no available patch

The Joomla Vulnerable Extensions List records extensions with known vulnerabilities for which no fix is available. For these, the Joomla Project's guidance is to uninstall the extension, not to wait for an update. Entries recorded during July and August 2026 include:

- JEM - five issues, no stable fix at time of writing
- EasyStore Pro 2.0.1
- Phoca Maps, versions prior to 6.1.0
- Phoca Guestbook
- DJ-Classifieds
- Gridbox 2.2

The Vulnerable Extensions List is updated continuously. Organisations should consult it directly at vel.joomla.org rather than relying on this advisory as a complete or current record. A separate resolved list records extensions for which a fix has since been issued, including ChronoForms, resolved in version 8.0.53.

What does this mean?

An outdated extension provides the initial foothold, a webshell is installed for persistence, and the web server is then used as a staging point against systems it can reach.

Two practical difficulties make this class of risk harder to manage than core patching. Most site owners cannot readily say which extensions are installed on their site, particularly where the site was built by a contractor some years ago. And updating an extension does not remove an attacker who is already present, so a site compromised before patching remains compromised afterwards.

Mitigation process

CERTVU recommends the following:

1. **Inventory Your Joomla Sites and Extensions**

Identify every Joomla site your organisation operates, including sites maintained by an external web developer or hosting provider. For each, log in to the Joomla administrator and open Extensions, then Manage, then Manage, to list every installed extension and its version. Record the result; this inventory is the prerequisite for everything else in this advisory.

2. **Update Joomla Core**

Update to Joomla 6.1.3 or 5.4.8 as appropriate to the branch in use, using the built-in Joomla Update component.

Other mitigating options include:

- Update or Remove Extensions
- Disable Unused Webservices
- Restrict Administrative Access
- Assess for Prior Compromise
- Establish an Ongoing Process

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

Reference

1. https://www.joomla.org/announcements/release-news/joomla-6-1-3-5-4-8-security-bugfix-release.html
2. https://developer.joomla.org/security-centre.html
3. https://vel.joomla.org/
4. https://www.cve.org/CVERecord?id=CVE-2026-48907
5. https://www.cve.org/CVERecord?id=CVE-2026-48904
6. https://www.cisa.gov/known-exploited-vulnerabilities-catalog