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

4 September 2026

Advisory 255: JobSearch WP Job Board Plugin Unauthenticated PHP Object Injection (CVE-2026-84834).

Release Date: 3rd September 2026
Impact: 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, System/Network administrators, and website/HR teams that operate a WordPress site using the JobSearch (eyecix) job board plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84834 is a critical, unauthenticated PHP Object Injection vulnerability in JobSearch, a commercial WordPress job-board plugin by eyecix sold on the Envato CodeCanyon marketplace, with over 2,640 recorded sales and a 4.5-star rating across 260 reviews, used by organizations to publish job listings and manage employer/candidate applications on their own WordPress sites. The flaw allows an attacker to submit specially-crafted serialized PHP data that the plugin deserializes without validating its origin or type. If the WordPress installation (core, another plugin, or a theme) contains a suitable "gadget chain".

What are the systems affected?

The following version(s) are affected:

- JobSearch through 3.2.0 - (Affected)

A version after 3.2.0 that addresses this CVE – (see “Mitigation process” below to confirm)

What does this mean?

Typical attack flow:

1. **Submit crafted serialized PHP data to a vulnerable endpoint**
   - An unauthenticated attacker sends a specially crafted, serialized PHP object as part of a request to a WordPress site running an affected version of JobSearch, targeting a code path that deserializes attacker-supplied input without validating its origin or type.
2. **Trigger a gadget chain during deserialization**
   - If the WordPress installation — core, another installed plugin, or the active theme — contains a class with a magic method (such as __destruct() or __wakeup()) that performs a dangerous action when instantiated, PHP’s deserialization process automatically invokes it, potentially resulting in arbitrary file deletion, denial of service, or remote code execution depending on the specific gadget chain available on that site.

Attack vectors:

- A network-based, unauthenticated request against any internet-reachable WordPress site running an affected version of the JobSearch plugin.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the vulnerability requires no authentication at all, and the practical severity of a successful exploit depends on what other plugins and themes are installed on the same site.

Successful exploitation may allow attackers to:

- Trigger arbitrary file deletion or a denial-of-service condition on the affected WordPress site, without ever holding a legitimate credential.
- Depending on the specific combination of plugins, themes, and WordPress core version installed on the site, potentially achieve remote code execution via an available deserialization gadget chain, resulting in full site compromise.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update the JobSearch plugin to the latest available version through the WordPress admin dashboard (Plugins > Installed Plugins), and confirm via the vendor’s own changelog (eyecix / CodeCanyon item page) that the update addresses this PHP Object Injection issue.

2. Treat this as urgent given the unauthenticated, no-privilege-required nature of the flaw and the plugin's prior history of vendor-acknowledged vulnerabilities
3. Audit the estate for JobSearch installations
4. Consider a Web Application Firewall (WAF) as an interim layer of defence
5. Review web-server access logs for suspicious activity

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-84834
2. https://codecanyon.net/item/jobsearch-wp-job-board-wordpress-plugin/21066856