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 257: Mail Mint (WPFunnels) Unauthenticated PHP Object Injection (CVE-2026-84753).

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 marketing/website teams that operate a WordPress or WooCommerce site using the Mail Mint email marketing automation plugin by WPFunnels. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84753 is a critical, unauthenticated PHP Object Injection vulnerability in Mail Mint, a WordPress email marketing, newsletter, and automation plugin by WPFunnels with over 4,000 active installations and a 4.7-star rating, used to send WooCommerce transactional emails and run automated marketing campaigns. The flaw allows an attacker to submit specially-crafted serialized PHP data that the plugin deserializes without validating its origin or type.

What are the systems affected?

The following version(s) are affected:

- Mail Mint through 1.31.0 - (Affected)

Mail Mint 1.31.1 and later - (Not affected, patched)

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 Mail Mint, 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 Mail Mint 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, and access subscriber/contact data managed by Mail Mint's email marketing functionality.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update the Mail Mint plugin to version 1.31.1 or later through the WordPress admin dashboard (Plugins > Installed Plugins), and confirm via the plugin's own changelog 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 this plugin's extensive history of prior, separately-patched vulnerabilities
3. Audit the estate for Mail Mint 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-2026-84753
2. https://wordpress.org/plugins/mail-mint/