

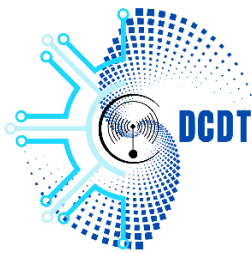
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

3 September 2026

Advisory 249: UnoPim Authenticated Arbitrary File Upload Leading to Remote Code Execution (CVE-2026-82524).

Release Date: 2nd September 2026

Impact: **HIGH**

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 e-commerce/retail IT teams that deploy or operate UnoPim as a self-hosted Product Information Management (PIM) platform. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-82524 is a high-severity authenticated file upload vulnerability leading to remote code execution in UnoPim, an open-source Product Information Management (PIM) platform built on Laravel that organizations use to centrally manage and enrich product data, including catalogs of over 10 million products across multiple sales channels. The flaw is in UnoPim's TinyMCE image upload endpoint, which is missing proper file extension and MIME type validation. An authenticated administrator-level user can abuse this endpoint to upload an arbitrary PHP web shell to the application's public storage disk, then execute arbitrary operating-system commands on the server simply by accessing the uploaded file at the URL the server itself returns in its response.

What are the systems affected?

The following version(s) are affected:

- UnoPim before 2.1.5 - (Affected)

UnoPim 2.1.5 and later - (Not affected, patched)

UnoPim is typically self-hosted rather than centrally auto-updated by the vendor, so this fix will not reach an existing deployment on its own. Organizations should confirm the running version directly via the UnoPim admin console or deployment configuration.

What does this mean?

Typical attack flow:

1. **Upload a malicious PHP file via the TinyMCE image upload endpoint**
 - An attacker who already holds administrator-level credentials to a reachable UnoPim instance uses the TinyMCE image upload endpoint which does not properly validate file extension or MIME type to upload a PHP web shell disguised as an image to the application's public storage disk.
2. **Access the uploaded file to execute arbitrary commands**
 - The attacker retrieves the URL to the uploaded file from the server's own response and accesses it directly, causing the PHP web shell to execute and giving the attacker the ability to run arbitrary operating-system commands on the underlying server.

Attack vectors:

- Requires the attacker to already hold administrator-level credentials to a reachable UnoPim instance (CVSS PR:H) - this is not exploitable by an anonymous, unauthenticated attacker with no account.
- No user interaction is required beyond that authenticated access (CVSS UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the technical details and a proof-of-concept-style researcher writeup are now public, and the practical impact of a successful attack (full server-side remote code execution) is severe.

Successful exploitation may allow attackers to:

- Execute arbitrary operating-system commands on the server hosting UnoPim, achieving full remote code execution.
- Access, exfiltrate, or tamper with the product catalog and any other data managed through UnoPim, and use the compromised server as a foothold into other systems on the same network.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade UnoPim to version 2.1.5 or later, where this vulnerability is fixed as part of the vendor's own file-upload security hardening. Because UnoPim is self-hosted, this requires a deliberate upgrade - confirm the running instance has actually reached the fixed version.

2. Review which accounts hold administrator-level access to UnoPim, since this vulnerability can only be exploited by an already-authenticated administrator
3. Audit the estate for UnoPim deployments
4. Treat any unpatched instance with untrusted administrator access as potentially compromised
5. Rotate credentials and review uploaded files

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-82524>
2. <https://github.com/unopim/unopim/releases/tag/v2.1.5>