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

31 August 2026

Advisory 210: xShop Admin Panel Unrestricted File Upload Remote Code Execution Vulnerability (CVE-2026-49849).

Release Date: 21st August 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 self-hosting the xShop e-commerce platform and to the developers and administrators who manage it. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-49849 is a critical unrestricted file upload vulnerability in xShop, an open-source, self-hosted e-commerce platform built on Laravel. The flaw lies in the admin panel's file attachment module, which fails to properly restrict the type of file an authenticated administrator can upload, allowing a PHP script to be uploaded and stored in a location the web server will execute.

Exploitation requires an attacker to already hold administrator-level access to the xShop admin panel. Once a malicious script is uploaded, the attacker gains remote code execution on the underlying server, turning an admin-panel compromise into complete server compromise.

What are the systems affected?

The following software and version(s) are affected:

- xShop (self-hosted, open-source Laravel e-commerce platform), version 3.0.3 – (Affected)

xShop version 3.0.4 and later – (Not affected, patched)

There is no evidence of active exploitation at the time of this advisory. The vendor (4xmen) has already published a fixed release, v3.0.4, on GitHub.

What does this mean?

Typical attack flow:

1. **Attacker obtains administrator-level access**
    - The attacker gains admin-panel access through means such as stolen or phished credentials, a rogue insider, or by chaining this flaw with a separate credential-theft vulnerability. This CVE does not itself grant that initial access.
2. **Attacker uploads a malicious script via the file attachment module**
    - The attacker uploads a file with a dangerous extension, such as a PHP script, which the file attachment module does not properly restrict or validate.

Attack vectors:

- A malicious or compromised administrator account
- An attacker who has phished or otherwise obtained valid admin credentials

Successful exploitation allows attackers to:

- Execute arbitrary code on the underlying server with the privileges of the web server process
- Achieve complete system compromise — reading or modifying the database, stealing customer and payment data, and using the server as a foothold for further attacks

Mitigation process

CERTVU recommends the following:

1. Upgrade to xShop v3.0.4 Immediately
The vendor (4xmen) has released a fixed version, v3.0.4, on GitHub, which corrects the file attachment module's upload validation.
Treat this as an emergency change given the CVSS 9.1 rating and the potential for complete server compromise.
2. Restrict Admin Panel Access
use IP allowlisting or a VPN, and enforce multi-factor authentication for all administrator accounts, since exploitation depends on an attacker first obtaining admin-level access.
Other mitigating options include;

- Audit for Signs of Compromise
- Harden Upload Directories
- Rotate administrator credentials as a precaution if compromise cannot be ruled out.

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-49849
2. https://github.com/4xmen/xshop/security/advisories/GHSA-fc35-qjg3-f6g7