CHECKLIST · SCAMS & SECURITY

A fake photo upload could take over your website. Check your server

Published 23 November 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/ghostscript-upload2shell-image-upload-flaw/

- [ ] **Check your WordPress version.** Go to Dashboard -> Updates. You need 7.0.4 or later, or the patched release for an older branch such as 6.9.7.
- [ ] **Ask your web host or IT provider about CVE-2026-125396.** Ask whether the server's Ghostscript package includes the fix, and when it was installed.
- [ ] **Rebuild containers and app bundles.** Any Docker image or app that ships its own Ghostscript needs rebuilding with 10.08.0 or a patched package.
- [ ] **Review public upload forms.** If Forminator or Essential Addons for Elementor lets signed-out visitors upload files, turn that off until the server is patched.
- [ ] **Put a password on shared print queues.** A Linux print server that accepts network jobs without a login should require one.
- [ ] **Switch off anonymous uploads on wikis.** The MediaWiki and DokuWiki attacks needed a wiki open to uploads from anyone. Require a login until Ghostscript is patched.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.