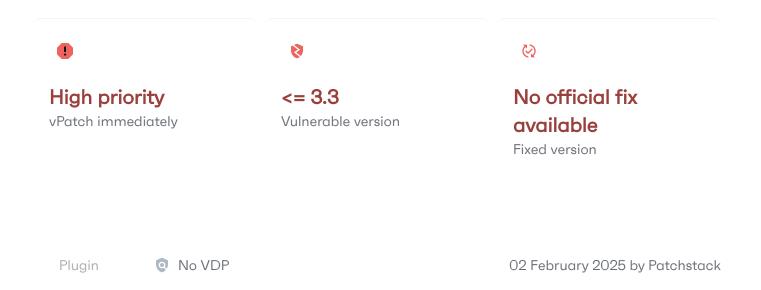
## WordPress Plugin A/B Image Optimizer Plugin <= 3.3 is vulnerable to Arbitrary File Download



## Risks cvss 7.5

This vulnerability is highly dangerous and expected to become mass exploited.

## 7.5 Arbitrary File Download

This could allow a malicious actor to download any file from your website. This includes but is not limited to files that contain login credentials or backup files.

This is a general description of this vulnerability type, specific impact varies case by case. CVSS score is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way, but it is not ideal for CMSs.

Pricing Login Start trial

We advise to mitigate or resolve the vulnerability immediately.

## Automatically mitigate vulnerabilities and keep your websites safe

Patchstack has issued a virtual patch to mitigate this issue by blocking any attacks until an official fix becomes available, can be tested and be safely applied.

Get the fastest vulnerability mitigation with Patchstack! Get Started

_			
	$\sim$	en i I	
ப	eu		15

Expand full details

Have additional information or questions about this entry? Let us know.

Pricing Login Start trial

- Reported by LVT-tholv2k 26 Jan 2025
- 1 Published by Patchstack 02 Feb 2025

Go to Plugin page Q No VDP

How can Patchstack provide the fastest protection?

Patchstack is one of the largest open-source vulnerability disclosers in the world.

\*\*OF EXAMPLE, The 2023 incore than 70% of new WordPress vulnerabilities were originally published by Patchstack. This focus on research enables us to deploy Patchstack Patchstack. This focus on research enables us to deploy Patchstack Patchstack accurity vulnerabilities even when there's no which be the fastest and most effective way to eliminate new security vulnerabilities without sacrificing performance. Hackers automate attacks against new security vulnerabilities to take over as what we see the sets the content of the fastest are opportunistic and victims are not chosen - everyone is a target. We recommend reaching out to your hosting provider for server-side malware scanning or use a professional incident response service. Don't rely on plugin based malware scanners as they are commonly tampered with by malware.

Weekly WordPress security intelligence delivered to your inbox.

Website security For plugin devs For researchers Resources Patchstack Managed VDP Vulnerability Database Pricing Bug bounty About For WordPress Whitepaper 2024 Careers Log in NEW Log in NEW WordPress Statistics NEW For WooCommerce Affiliates **NEW** Active programs Guidelines For agencies Security auditing Case studies **NEW** Merch store Learn **NEW** API For hosts Media kit Discord Articles

Documentation

FAQ

Log in

Socials

LinkedIn

Facebook

X

Pricing Login Start trial