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

High priority
vPatch immediately

<= 3.3
Vulnerable version

No official fix available
Fixed version

Plugin

No VDP

02 February 2025 by Patchstack

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.

We advise to mitigate or resolve the vulnerability immediately.

Details

Expand full details

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

Reported by LVT-tholv2k
26 Jan 2025

Published by Patchstack
02 Feb 2025

Go to Plugin page

No VDP

How can Patchstack provide the fastest protection?

Patchstack is one of the largest open-source vulnerability disclosers in the world. For example, in 2023 more than 70% of new WordPress vulnerabilities were originally published by Patchstack. This focus on research enables us to deploy vulnerability protection rules faster than anybody else.

What is virtual patching?

Patchstack vPatching auto-mitigates security vulnerabilities even when there's no official patch available. It's the fastest and most effective way to eliminate new security vulnerabilities without sacrificing performance.

Why would a hacker target my website?

Hackers automate attacks against new security vulnerabilities to take over as many websites as they can before users have time to patch and update. The attacks are opportunistic and victims are not chosen - everyone is a target.

What if my website has already been compromised?

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.

Website security

- Pricing
- For WordPress
- For WooCommerce
- For agencies
- API For hosts
- Documentation
- FAQ
- Log in

For plugin devs

- Managed VDP
- Log in NEW
- Active programs
- Security auditing

For researchers

- Bug bounty
- Log in NEW
- Guidelines
- Learn NEW
- Discord

Resources

- Vulnerability Database
- Whitepaper 2024
- WordPress Statistics NEW
- Case studies NEW
- Articles

Patchstack

- About
- Careers
- Affiliates NEW
- Merch store
- Media kit

Socials

- LinkedIn
- Facebook
- X

European Innovation Council
Co-funded by the European Union