

[Pricing](#)[Case studies](#)[Login](#)[Start trial](#)

# WordPress Download Monitor Plugin $\leq 4.4.6$ is vulnerable to Arbitrary File Download



## Low priority

No impactful threat



$\leq 4.4.6$

Vulnerable version(s)



4.4.7

Patched version

 WordPress plugin

 Active VDP

29 Oct, 2021

Get the fastest vulnerability mitigation with Patchstack!

Get started

## Risks CVSS 6.8

Vulnerabilities like this one are used in mass-exploit campaigns. Attackers use these to attack thousands of websites at a time, regardless of traffic size or popularity.

[Pricing](#)[Case studies](#)[Login](#)[Start trial](#)

As immediate action, update the affected plugin. If you're unable to do so, ask your hosting provider or web developer for help.

## 6.8 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.

CVSS score is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way but which is not ideal for WordPress.

## Solutions

This security issue has a low severity impact and is unlikely to be exploited.

### Update to version 4.4.7 or later.

Update to version 4.4.7 or later to resolve the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.











## Details

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Type	Plugin
Vulnerable versions 	<= 4.4.6
Patched in 	4.4.7
OWASP Top 10 	A3: Sensitive Data Exposure
Classification 	Arbitrary File Download
CVE ID 	<a href="#">CVE-2021-31567 ↗</a>
Patchstack priority 	Low
CVSS severity 	6.8
Required privilege 	Administrator
Developer	<a href="#">WP Chill ↗</a>
PSID 	2da154895981
Credits	 <a href="#">RE-ALTER</a>
Published	29 Oct, 2021

[Vulnerability details ↗](#) [Vulnerability details ↗](#)

[↗ Expand full details](#)

Pricing

Case studies

Login


Start trial

Go to

WordPress plugin

Active VDP

## Timeline

Reported by  **RE-ALTER**  
NaN undefined, NaN

### Vulnerability mitigation

Pricing

Application security (SCA)  
How can Patchstack provide the fastest protection? ▼  
RapidMitigate **NEW**

Threat Intelligence (API)  
How does Patchstack mitigate vulnerabilities? ▼  
VS Monarx

VS Imunify360  
Why would a hacker target my website? ▼  
VS Wordfence

Documentation  
What if my website has already been compromised? ▼

Service status

Log in

### Code security

Managed VDP **NEW**

Active VDP directory **1,178**

Security auditing

Compliance (CRA) **NEW**

Weekly WordPress security intelligence delivered to your inbox.

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

## Bug bounty

[Bug bounty](#)

[Leaderboard](#)

[Guidelines](#)

[Learn](#) NEW

[Report](#)

[Discord](#)

[Log in](#) NEW

## Use cases

[Web developers](#)

[Webhosts](#) NEW

[Software vendors](#)

[WordPress](#)

[WooCommerce](#)

## Resources

[Partners](#)

[Vulnerability database](#)

[Whitepaper 2026](#) NEW

[Articles](#)

[Case studies](#) NEW

[Webinars](#) NEW

[Vulnerability statistics](#)

## Patchstack

[About](#)

[Careers](#)

[Merch store](#)

[Media kit](#)

[LinkedIn](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)