State of WordPress Security In 2022

01 Introduction
About Patchstack

02 WordPress security by the numbers
Most common WordPress security bugs in 2022
Most exploited WordPress security bugs in 2022

03 2022 WordPress core security updates
Unpatched WordPress core vulnerabilities from 2022

04 Biggest WordPress security trends from 2022
Unpatched security bugs are a silent security risk
Unsupported plugins
How Patchstack is addressing the unsupported plugin issue
Security issues in the software supply chain
Hosting companies are taking action

05 Patchstack section / what we’re doing
The security researcher community is growing
147 vulnerabilities escalated to the WordPress team

06 What to expect from 2023

07 Further reading and listening
Introduction

In this whitepaper, we will go over the biggest statistics and trends in WordPress ecosystem security in 2022. We will also offer a few pieces of advice to people building sites with WordPress.

The main highlights from the year 2022 are the risk of using abandoned or poorly maintained plugins and themes, and a broader concern with security issues in the open-source supply chain.

The theme of this whitepaper is one of responsibility – how every member of the WordPress ecosystem can contribute to making the internet safer. In this spirit, we’ll start off the paper with two pieces of advice – one for WordPress website developers, and one for plugin/theme makers.

If you’re a WordPress website developer, please be mindful of the plugins and themes you use in your sites. Through the years we’ve seen a lot of security issues arising from nulled, outdated, and abandoned components.

Consider this fact – in 2022, we found that **26% of plugins with critical security bugs never received a patch**. This means that any sites running those components are vulnerable to attacks. This number has sadly remained steady over the past few years.

If you’re a plugin/theme developer, pay attention to the libraries you are using in your own projects, and whether these are getting updates - particularly, security updates.

A security bug one library can impact hundreds of plugins and countless websites – as was the case in 2022 with a (now patched) security bug in the popular Freemius framework.

Both issues lead to the same conclusion, and advice - everyone, from site builders to plugin developers - should know what building blocks they rely on in their work.

Or, in short – patch your stack.

About Patchstack

Patchstack is a WordPress security maintenance & management tool for builders.

We offer websites protection against WordPress core, plugin, and theme vulnerabilities. Patchstack also owns the leading WordPress vulnerability database, runs the first bug bounty program for WordPress plugins, and offers an mVDP program.

Patchstack also provides a threat intelligence feed to WordPress hosting services, including Plesk, Hostinger, Pagely, and many more.
100% more security bugs reported in WordPress plugins in 2022.

In 2022, we saw 328% more security bugs reported in WordPress plugins – we added 4,528 confirmed security bugs to our database, compared to 1,382 in 2021. This is the highest number of security bugs we have ever confirmed.

The number of WordPress plugins increased by 27.2% in 2022, leading to an overall increase of 20.8% compared to 2020. The number of security bugs increased by 25% compared to 2020, reaching a total of 672.3% of the number of security bugs we saw in 2019.

According to the Cross-Site Scripting (XSS) plugin, WordPress plugins in 2022.

WordPress security by the numbers

On average, 42% of WordPress sites have at least one vulnerable plugin installed.

Most popular WordPress plugins in 2022

On average, 42% of WordPress sites have at least one vulnerable plugin installed.
2022 WordPress core security updates

The WordPress core team published 4 security releases in the project in 2022. These four releases addressed 26 security bugs in total, the most severe of which was a framework security enhancement.

The patch for aforementioned CVE-2022-21661 (Described as improper sanitization in WP_Query) protects plugin developers from creating SQL injection bugs, by ensuring all data is properly sanitized before it reaches the database.

Unpatched WordPress core vulnerabilities from 2022

The 26 patched security bugs do not include 2 unpatched security bugs reported publicly in WordPress core in 2022. These two unpatched security bugs that got full disclosure are low-risk concerns, and are described below:

Full disclosure is the practice of publishing or widely disseminating information about vulnerabilities so that potential victims are as knowledgeable as those who may attack them.

CVE-2022-3590 – Unauthenticated Blind SSRF

On September 5th, 2022, the respectable security researchers at InformSource released details regarding an Unauthenticated Blind SSRF security bug that went unpatched in WordPress core. The post includes a timeline that shows the researchers waited 228 days from their initial report before publicizing details.

The official severity assigned to CVE-2022-3590 by NVD (National Vulnerability Database) is a “5.9” Medium. In practicality, this may be too high. In order to perform the attack against a live website, attackers would first need to control the DNS (Domain Name System) server the Web Hosting server uses. This is a very unlikely scenario for most WordPress websites.

CVE-2022-33994 – XSS via SVG in Gutenberg

On July 30th, 2022 details of a potential stored XSS (Cross Site Scripting) security bug in how Gutenberg (WordPress’s editor) handles SVG (Scalable Vector Graphics) images were made public. This full disclosure came after 45 days of discussion between the security researchers and the WordPress core security team. The WordPress core team decided the report was informational and is having a discussion related to this issue in public tickets.

This CVE’s severity rating is a 3.0 or Low risk according to NVD. This is due to the fact the XSS payload will not be executed within the context of the WordPress application. This bug poses no risk to the WordPress website unless it was seriously misconfigured, however, most popular web application vendors have prevented similar SVG-related XSS bugs in their applications.
Unpatched security bugs are a client security risk

In 2022, 26% of new critical vulnerabilities did not receive a patch. This is a critical vulnerability in a trade-off happening in software development. Significant deficiencies in some open-source projects are putting users at risk.

The majority of that trend thought to be open-source software projects. This is because open-source projects have more frequent releases and more frequent updates compared to proprietary software.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did the OWASP Project contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?

The OWASP Project has been tracking vulnerabilities since 2002. They have reported that 26% of new critical vulnerabilities did not receive a patch in 2022.

Unpatched plugins

Security bugs are the most critical risk for our clients. By unpatched vulnerability risk, it is the slow to receive a patch. A critical vulnerability in a trade-off happening in software development.

Significant deficiencies in some open-source projects contribute to this risk. The majority of that trend thought to be open-source software projects.

A vulnerability in a security patch made available in late 2022 was revealed. This makes it difficult for security patches to be delivered.

Furthering the trend is a project called the OWASP Project, reporting on the public record of software security.

How exactly did OWASP contribute?
The security researcher community is growing

Patchstack Alliance is a bug bounty platform that helps security researchers find vulnerabilities. Our goal is to make it easier for researchers to submit vulnerability reports to developers, and for developers to have an easier time managing security issues.

In 2022, we paid $16,050 in bug bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities. In 2022 we paid $16,050 in bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities.

In 2022, we paid $16,050 in bug bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities. In 2022 we paid $16,050 in bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities. In 2022 we paid $16,050 in bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities. In 2022, we paid $16,050 in bug bounties to ethical hackers for valid bug reports. Our researchers reported 147 unique security vulnerabilities.
What to expect from 2023

Based on our observations, we are very optimistic about the upcoming year. Over the past three years, the WordPress ecosystem has grown a lot safer. The fact that we are seeing increased number of security bugs being fixed in plugins does not mean that suddenly there are more security bugs - what it means is that security bugs that have existed in the plugins for years are finally being addressed. We expect the same trend to continue in 2023.

We see the topic of security in open-source software becoming much more important. The [Securing Open Source Software Act of 2022](https://patchstack.com/database/the-state-of-wordpress-security-in-2023) recently introduced by the US is a clear sign that in the upcoming years, open-source vendors and companies relying on open-source software will need to implement more mature security practices.

Finally, and most importantly, we will continue to see an increased security awareness within the entire WordPress ecosystem. With the demand going up, we can expect to see better security provided by hosting companies, plugin developers and by website developers.

References

https://patchstack.com/database/
https://www.sanarec.com/blog/wordpress-core-unauthenticated-blind-srf/
https://wordpress.org/plugins/advanced-authentication/advanced-authentication/
https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/
https://wordpress.org/news/2022/03/wordpress-6-0-2-security-maintenance-release/
https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
Further reading and listening

Security community

Join our Facebook Community and get help, recommendations, and solutions for WordPress security from fellow community members.

Patchstack Weekly

Patchstack Weekly is a series hosted by Robert to catch up on recent events in open-source security, with an initial focus on WordPress.

Security insight

Browse our collection of security-related articles with tips to improve your security hygiene.