

Open-source security whitepaper • Data updated 15.02.2023

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

01

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 Through the years we’ve seen a lot of security issues arising from nulled, outdated, and abandoned components.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.



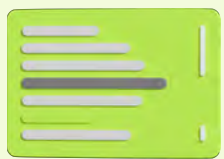
WordPress vulnerability management tool ↗

Identify and protect applications against known vulnerabilities in WordPress core, plugins, and themes.



Alliance bug bounty platform ↗

A security bug hunting platform connecting ethical hackers with open-source software developers.



Vulnerability database ↗

The free WordPress vulnerability database so enterprises and hosts can protect their customers.



Managed Vulnerability Disclosure Program ↗

Streamlined security bug reporting between security researchers and open-source software developers.

02

WordPress security by the numbers

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**.

The vast majority of the security bugs were found in plugins (93%). Themes accounted for 6.7% of bugs and only 0.6% were in the WordPress core platform itself.

This doesn't mean that WordPress is unsafe, or that plugin developers are getting sloppier - rather, the security researchers are looking harder and farther.

This also means that the WordPress ecosystem is becoming more secure because a lot more of these security bugs are being addressed and patched.

328% more security bugs reported in WordPress plugins in 2022.

Most common WordPress security bugs in 2022

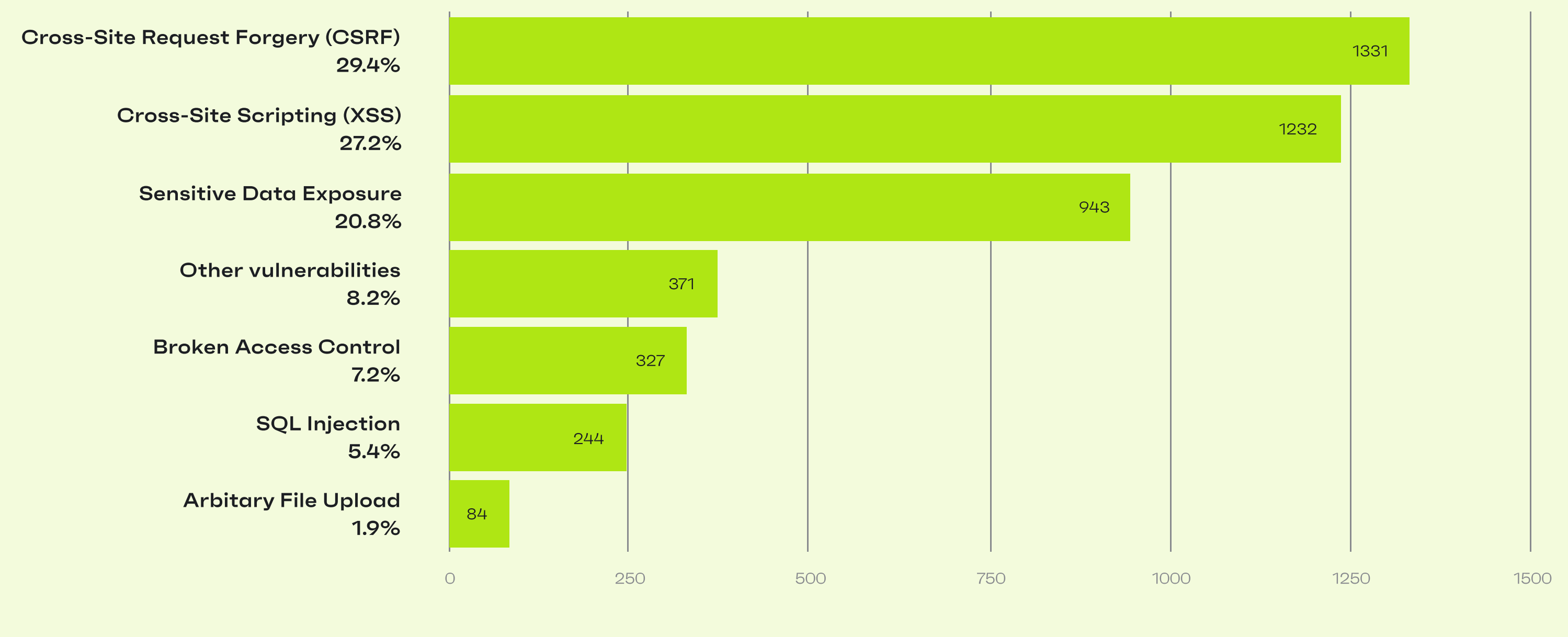
In previous years Cross-Site Scripting (XSS) has been the most common security bug reported, but in 2022 it was narrowly edged out by Cross-site Request Forgery (CSRF).

CSRF made a huge jump – when in 2021 it made up 11% of reported bugs, then last year it was 29%. There are a couple of reasons for that.

Firstly, CSRF is generally easier to find and thus they are reported more often. Secondly, last year a CSRF bug was found in the **Freemius framework** which affected a large number of plugins. Consequently, the number of CSRF bugs also increased dramatically.

Most common security bugs in WordPress in 2022

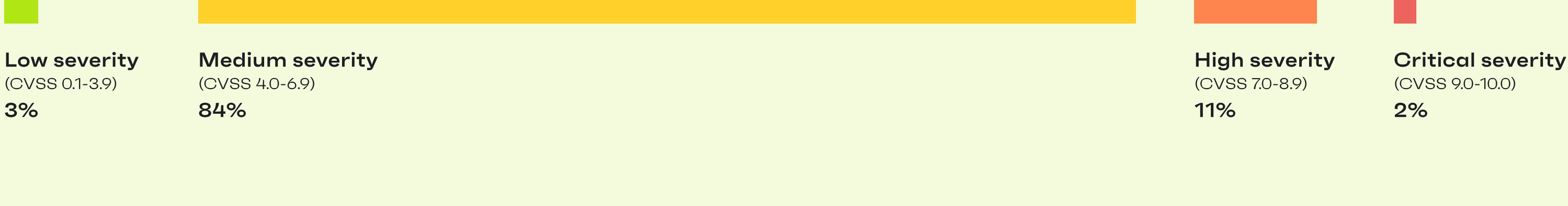
patchstack



Not all bugs are created equal – how big of a risk they pose depends on many different factors. Based on these each verified security bug is assigned a CVSS score on a scale of 10, with 10 representing critical severity.

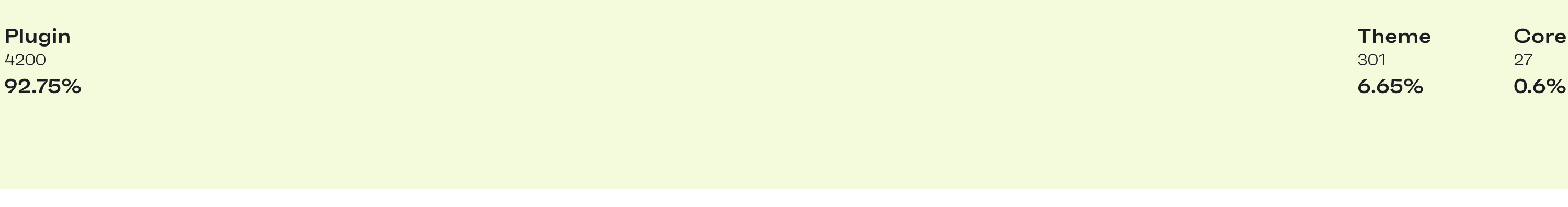
2022 WordPress security bug breakdown by severity

patchstack



2022 WordPress security bug breakdown by software type

patchstack



Popular plugins with reported security bugs

These were the most popular plugins containing a security bug, defined as having at least 1 million installs and at least one bug.

Only five of the plugins contained a high severity bug, and none contained a critical one.

Two of the highest CVSS score vulnerabilities were found in plugins related to Elementor. In 2022 we found security bugs in four other page builders. Most page builders are premium plugins and thus harder to access for security auditing, which explains the relatively small number of security bugs reported in them.

However we'd like to emphasise that even if you're using page builders to develop sites, you should still be mindful of the tools you use, and perform regular updates.

	Elementor Website Builder Theme	5+ million Installs	2 Security bug	8.8 Highest CVSS
	Essential Addons for Elementor Plugin	1+ million Installs	2 Security bugs	8.6 Highest CVSS
	UpdraftPlus WordPress Backup Plugin	3+ million Installs	1 Security bug	8.5 Highest CVSS
	One Click Demo Import Plugin	1+ million Installs	1 Security bug	7.2 Highest CVSS
	MonsterInsights Plugin	3+ million Installs	1 Security bug	7.1 Highest CVSS
	WooCommerce Theme	5+ million Installs	4 Security bugs	6.6 Highest CVSS
	All-In-One WP Migration Plugin	5+ million Installs	2 Security bugs	6.6 Highest CVSS
	All in One SEO Plugin	3+ million Installs	1 Security bug	5.4 Highest CVSS
	Yoast SEO Plugin	5+ million Installs	1 Security bug	5.3 Highest CVSS
	WordFence Plugin	4+ million Installs	1 Security bug	4.4 Highest CVSS
	Contact Form by WPForms Plugin	5+ million Installs	1 Security bug	4.1 Highest CVSS

On average, 42% of WordPress sites have at least 1 vulnerable software installed.

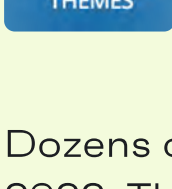

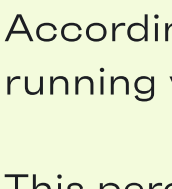
See if your website contains any vulnerable components

Sign up for free

Most targeted WordPress vulnerabilities in 2022

We analyzed our firewall activity logs to detect which vulnerabilities attackers target the most. The following is a ranking of the vulnerabilities based on how many exploit attempts were made against them.

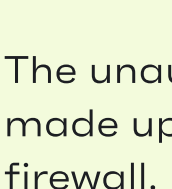

Top 3 new vulnerabilities with the most attempted exploits

	AccessPress Backdoor	Dozens of plugins and themes were compromised in a supply chain attack on AccessPress in early 2022. The vulnerability affected over 360,000 websites and it enabled attackers to use a backdoor to gain access to infected websites.
	Frontend File Manager Arbitrary File Upload	Versions 21.2 and older of this plugin were affected by an Arbitrary File Upload vulnerability. This could allow a malicious actor to upload any type of file to a website, including backdoors which are then executed to gain further access to a website. The vulnerability was patched in version 21.3. According to the WordPress repository, as of February, 8th, 2023, 56% of sites using this plugin are still running versions 21.2 and older, meaning that they are potentially vulnerable to attacks. This percentage of out-of-date versions highlights a bigger issue in the WordPress space of people not updating their sites often enough.
	School Management Pro Backdoor Arbitrary File Upload	Versions 99.6 and older of the School Management Pro plugin contained a backdoor that allowed Remote Code Execution. This could allow a malicious actor to execute commands on the target website and can be used to further gain access to the website in order to assume full control of it. This vulnerability has been fixed in version 99.7.

We also keep seeing attack attempts against older vulnerabilities.

There are open-source hacking tools available online which are made to automate attacks on scale. Many of them are made years ago and include exploits of known old vulnerabilities.

Old vulnerabilities still actively exploited (pre-2022)

	Social Warfare Unauthorized XSS/RCE	The unauthenticated XSS vulnerability in Social Warfare plugin was first reported in 2019 – last year it made up 97% of detected attempts against old vulnerabilities, based on data on hits made against our firewall.
	Duplicator Arbitrary File Download	Publicly disclosed in 2020, this vulnerability allowed an attacker to download files from an affected website, including those containing login credentials. In 2022, it only accounted for 2% of attempts made for old plugins

In general, however, few old vulnerabilities get active exploit attempts – over time sites update or remove vulnerable plugins, which in turn makes it harder for the attacker to find a website that can be exploited. For an attacker this may not be worth it if the success rate starts dropping significantly.

03

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.

WordPress [announced](#) the end of security updates for versions 3.7 through 4.0 on September 7, 2022. This affected less than 1% of total installations, and users now receive a very prominent warning in their website's wp-admin dashboard.

5.8.3 security release	5.9.2 security release	6.0.2 security release	6.0.3 security release
4 Security bugs patched Jan 6, 2022	3 security bugs patched Feb 22, 2022	4 security bugs patched Aug 30, 2022	16 security bugs patched Oct 11, 2022

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 [Sonar Source](#) 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.

04

Biggest WordPress security trends from 2022

Unpatched security bugs are a silent security risk

When we looked at the most critical security bugs disclosed in 2022, **we found that 26% never received a fix.**

Most of the time abandoned and unsupported plugins are removed from the [WordPress.org](#) directory - but any such plugins that are installed on websites will stay there until deleted by people running those sites.

We have talked about the [risks of using abandoned plugins and themes](#) before. Such plugins are dangerous because they are a potential threat even if the site has auto-updates enabled. A vulnerable and abandoned plugin would give no indication to the user that something is wrong - with no available updates it would look as if everything were up to date.

Furthermore, if a plugin is removed from the WordPress plugin repository, the public record of its security issues is lost.

26% of new critical vulnerabilities did not receive a patch in 2022.

Protect your websites against unpatched vulnerabilities with Patchstack

[Sign up >](#)

Unsupported plugins

Security bugs are just bugs that can be patched. A security bug becomes a vulnerability if a site does not receive a patch. If that vulnerability is exploited it leads to sites being compromised. Notifications about insecure components inform users to patch, preventing the compromise from happening.

The majority of bugs reported through the Patchstack Alliance in 2022 received a timely patch from the developer. However, not all reports lead to patches. In some cases, the insecure component received no patch and was subsequently removed from its respective repository. The closure of 87 themes/plugins in 2022 was directly related to their inability to address a security bug.

An unfortunate truth is that software available in public repositories is sometimes unsupported due to it being abandoned. This problem is exacerbated by the fact website owners will see a misleading "no update available" for these insecure components. Many site owners are simply unaware they are running insecure and unsupported components.

Using a vulnerability assessment tool like the [Patchstack app](#) or [Patchstack Threat Intelligence](#) feed can help identify components with known security bugs in them, empowering site owners to take action to secure their sites before they are hacked.

How Patchstack is addressing the unsupported plugin issue

Last Patch tutorial series

In a series of experimental posts, the Patchstack team provided a security review and shared patches for 6 plugins that were closed due to security issues. Each of these posts highlights a different security vulnerability and shares insight into how a defensive developer can address each security bug easily.

Curious to learn how we patch vulnerabilities?

[See tutorials >](#)

mVDP (Managed Vulnerability Disclosure Policy)

In an effort to improve communication between security researchers and open-source developers, we released the public beta for our managed Vulnerability Disclosure Policy or mVDP system in late 2022.

The mVDP provides value to both developers and security researchers. When a developer registers a security point of contact with Patchstack, we will know exactly who to reach out to if we receive a security bug report affecting one of their projects. In turn, Patchstack reviews security bug reports for the project, and rejects any invalid reports.

The mVDP program is **available for free for all FOSS** (Free Open-Source Software) plugins and themes. We ask for a reasonable annual fee from any paid, premium, or subscription-based plugins or themes to support this effort.

Get started with a vulnerability disclosure program for your plugin

[Free for FOSS >](#)

Security issues in the software supply chain

The global economy and open-source software have something in common. They both depend on a supply chain – the past year showed many of us what happens when supply chains break down. How life can be disrupted when individual links in these ephemeral chains are unsupported or fail, the outcomes can be unexpected.

Open source depends on a supply chain of code. We first saw the effects of security bugs in the open-source software supply chain in late 2021 with a vulnerability in **log4j**. This concern is not limited to just Java-based logging libraries though. In 2022 the WordPress ecosystem experienced vulnerabilities in multiple component supply chains, but it fared a lot better than log4j. Here is what happened and why.

Freemius framework vulnerability

Freemius is a popular SDK (Software Development Kit) used by hundreds of popular WordPress plugins and themes. In early 2022, there was a report of a low to medium-risk security bug found in the Freemius code. This spurred a monumental effort from the Freemius team and WordPress.org plugin repository volunteers. The almost thousand plugins that utilized Freemius needed to be informed to update their version of the Freemius libraries in their code base.

The good news was hundreds of plugins that were notified of the security bug in Freemius updated their project's code and patched the bug. The bad news was dozens of hundreds of projects did not respond to the notifications. These projects did not update their Freemius libraries, and in the end, were removed from the WordPress.org repository due to security concerns.

YITH framework vulnerability

A fully independent platform that sells plugins for WooCommerce shops, also independently develops all of its offered plugins using its own in-house framework. This central framework is a mature development practice, which lead to a smooth rollout when they faced a security bug.

A single, low to medium-severity security bug (CSRF) was identified in the shared code between many of the YITH plugins. The developers at YITH produced a patch in short order and deployed this patch downstream to dozens of their affected plugins.

The patch made available downstream was much faster for YITH compared to Freemius. This is because the Freemius library is used by many developers, while YITH's code libraries were only used in their own plugins. This a sign that security improves with fewer links in the overall software supply chain.

These examples have one common positive thing going for them. Each project was supported by its developers, and those developers were able to make a security patch available for all of the projects downstream that relied on their core code or framework.

If you run or manage a WordPress website, it is important to know what plugins and themes you rely on. The next time you apply a security patch, remember that the patch was made available by a developer somewhere upstream in your supply chain. Take a minute to acknowledge your reliance on their support and consider supporting those projects in turn.

[To support our Alliance bug bounty program, please reach out to us.](#)

[Learn more >](#)

Ecosystem leaders are taking action

Over the past year or so we've seen a very positive trend of more and more WordPress hosting services alerting their customers about vulnerabilities in their sites.

We've been working together with service providers to integrate our vulnerability feed to their systems in an effort to create an additional security layer for the WordPress ecosystem. A notable example of this is [One.com](#) – in one year **they fixed 56,000 vulnerabilities** on their customers' sites with the help of our intel feed and their own update management software.

Since late 2021, **17 hosting & service providers** have started using our threat intelligence feed to alert their customers. We want to extend our thanks to all of them for making the ecosystem safer:

05

Patchstack Alliance

The security researcher community is growing

Open-source security is a community effort.

Patchstack Alliance is our bug bounty platform that helps connect security researchers with plugin developers. 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.

Since creating the Alliance in 2021, we’ve grown our annual number of confirmed vulnerability reports more than seven times.

In 2022 we paid \$16,050 in bounties to ethical hackers for valid bug reports. Our researchers reported **748 unique security bugs**.

710 CVE IDs were reserved for those vulnerabilities – the number is smaller than the number of vulnerabilities reported due to some reports being merged upon inspection.

In 2022 we paid \$16,050 in bug bounties!

Join Patchstack Alliance and earn rewards for finding security bugs

Join the Alliance >

147 vulnerabilities escalated to the WordPress team

Whenever our researchers find a security bug, we first try to reach out to the developer of the plugin or theme and get them to resolve the security issue. Unfortunately, this is not always possible, and if the developer is unresponsive, we notify the WordPress team about the security bug.

In 2022 we asked the WordPress team to get involved in **147** cases. Of these, 60 bugs were subsequently patched by their developer.

The plugin with the largest installation base that we could not contact had over 800,000+ active installations. The developers patched the security bug only after the [WordPress.org team](#) notified them about it.

Of the 60 plugins that were escalated to the WordPress.org team, 31 had more than 10,000+ installs.

However, **87 security bugs went unpatched even after escalation**. These projects were likely abandoned and have been removed from the [WordPress.org](#) repository.

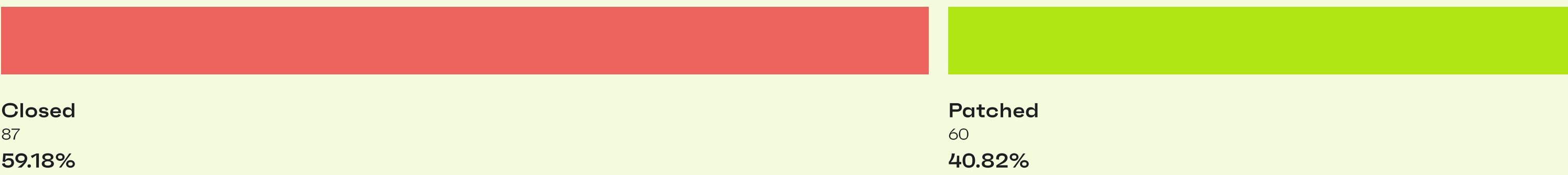
We encourage all plugin developers to be more open about security issues, and we recommend you have a vulnerability disclosure policy in place to make reporting security bugs easier. If you have stopped actively supporting a project, then you should let your users know.

Having a transparent approach to security is a sign of a mature approach to development, and it can be a trust signal for your users.

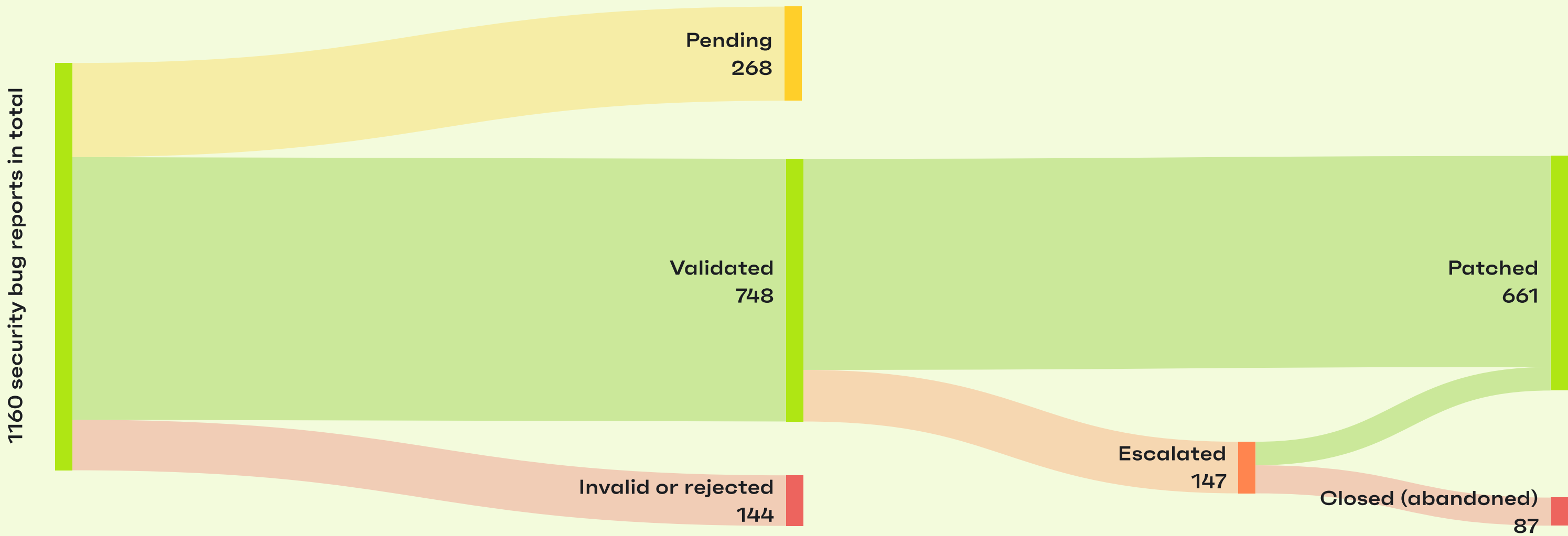
Status of vulnerabilities escalated to WP.org in 2022*



*By Patchstack Alliance



2022 Patchstack Alliance security report data



2022 Patchstack Alliance top contributors



Month	1st	2nd	3rd
January	Kim Jong Min	Ngo Van Thien	Rasi Afeef
February	Muhammad Daffa	Ngo Van Thien	Rasi Afeef
March	Muhammad Daffa	Nguy Minh Tuan	Tien Nguyen Anh
April	0xB9	ptsfense	Ngo Van Thien
May	Rasi Afeef	Muhammad Daffa	Rotem Bar
June	Muhammad Daffa	Muhammad Daffa	Rasi Afeef
July	Muhammad Daffa	Muhammad Daffa	Rasi Afeef
August	Muhammad Daffa	Lana Codes	Tien Nguyen Anh
September	Lana Codes	Muhammad Daffa	Tien Nguyen Anh
October	Lana Codes	Nguyen Anh Tien	TomS
November	Lana Codes	Mika	Muhammad Daffa
December	Lana Codes	Muhammad Daffa	Cat

06

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' 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://patchstack.com/whitepaper/the-state-of-wordpress-security-in-2021/>
<https://patchstack.com/articles/why-avoid-abandoned-wordpress-plugins-and-themes/>
<https://patchstack.com/database/vulnerability/school-management-pro/wordpress-school-management-pro-premium-plugin-9-9-7-unauthenticated-remote-code-execution-rce-via-rest-api>
<https://patchstack.com/database/vulnerability/nmedia-user-file-uploader/wordpress-frontend-file-manager-plugin-21-2-authenticated-arbitrary-file-upload-vulnerability>
<https://www.bleepingcomputer.com/news/security/over-90-wordpress-themes-plugins-backdoored-in-supply-chain-attack/>
<https://blog.jitendrapatro.me/cve-2022-33994-stored-xss-in-wordpress/>
<https://www.one.com/en/about/news/wordpress-vulnerabilities-repaired>
<https://www.sonarsource.com/blog/wordpress-core-unauthenticated-blind-ssrf/>
<https://wordpress.org/plugins/nmedia-user-file-uploader/advanced/>
<https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/>
<https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/>
<https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/>
<https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/>

Discover and protect against vulnerabilities in your web applications.

Check pricing and features >



07

Further reading and listening

Security community



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

[Join community >](#)

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.

[Listen on Spotify >](#)

Security insight



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

[Continue to articles >](#)