

Security whitepaper • Data updated 04.03.2022

State Of WordPress Security In 2021



01 Introduction

About Patchstack

02 WordPress core

Insecure PHPMailer library

Fear of dependency confusion attacks

WordPress.org vulnerability disclosure policy and bug bounty program

03 WordPress themes

Theme vulnerabilities are just as critical as plugin vulnerabilities

The trend of critical vulnerabilities in themes

04 WordPress plugins

Authorization Checks (or securing AJAX endpoints)

05 150% rise in vulnerabilities found compared to 2020

Cross-Site Scripting (XSS) Highly Prevalent

06 Fewer plugins are used while more of them are outdated

07 Easy to exploit vulnerabilities remain the main targets

08 Old vulnerabilities remain targeted

09 \$12,850 to ethical hackers for securing plugins

10 Increased awareness around vulnerabilities

11 Website security budgets are almost nonexistent

The biggest problem in WordPress security remains

12 Conclusion

Sources

13 Further reading and listening

01 Introduction

WordPress is the technology powering 43.2% of websites on the web in 2021, this is up from 39.5% at the end of 2020.

Vulnerabilities from plugins and themes remain as one of the biggest threats to websites built on WordPress. In fact, just 0.58% of security vulnerabilities originate from WordPress core in 2021.

We’ve seen a 150% growth in vulnerabilities reported in 2021 compared to 2020 which is a significant increase. Meanwhile, 29% of the WordPress plugins with critical vulnerabilities received no patch.

In 2021, Patchstack launched a bug bounty community of ethical hackers (Patchstack Alliance) to identify and patch vulnerabilities across the entire WordPress ecosystem. In 2021, around \$13,000 was paid out as bounties. **Brands such as Plesk, cPanel, Pagely, and many others are already supporting it. [Join the movement!](#)**


This whitepaper summarises the year 2021. We’ll be looking into WordPress core security in general, dive into plugin vulnerabilities, and explore the data we have gathered.

About Patchstack

Patchstack is leading the way in open-source security by connecting technology, threat intelligence, and community to secure the open-source ecosystem.


Patchstack is an officially authorized CNA to assign CVE IDs to WordPress-related vulnerabilities. Patchstack is also a winner of Global InfoSec Awards 2021 in two categories: Open Source Security and Web Application Security for providing "Cutting Edge" solutions to the market.

WordPress security ↗




Identifies known vulnerabilities in WordPress core, plugins, and themes to provide automated protection (virtual patching).

Alliance platform ↗



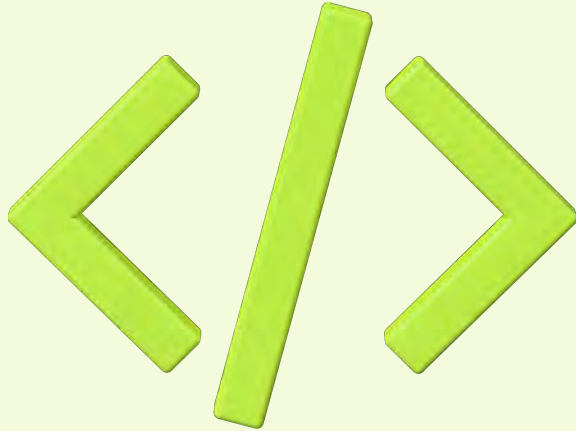
Our bug hunting platform connects ethical hackers with open-source vendors and helps keep open-source secure.

Vulnerability database ↗



We manage the free WordPress vulnerability database which hosting companies and enterprises can leverage to [protect their customers](#).

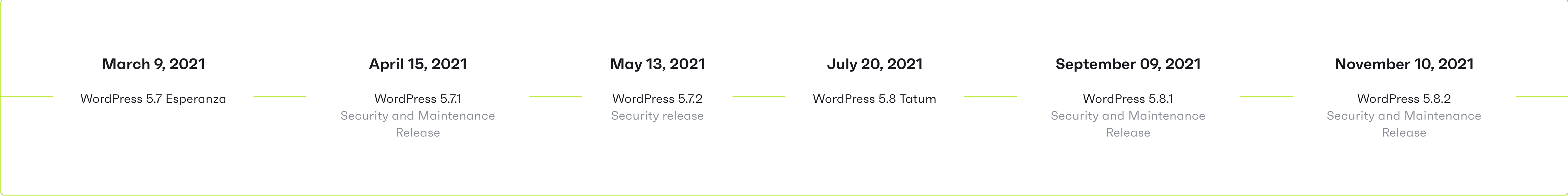
Security auditing ↗



We provide professional code review and security auditing to open-source software such as WordPress plugins and themes.

02 WordPress core

WordPress core is showing continuous improvements at regular intervals. There have been 4 security releases in 2021 - 5.7.1, 5.7.2, 5.8.1, and 5.8.2. Such a regular release schedule is a sign of a mature product.



Insecure PHPMailer library

Of those 4 security releases, only one contained a patch for a critical vulnerability. This sole critical vulnerability was not in WordPress logic either but was a security concern caused by insecurity found in an open-source component WordPress core was including.

This insecure component was the PHPMailer library, and WordPress core addressed this issue by updating that library. The PHPMailer library was affected by an object injection vulnerability (described in CVE-2020-36326) this vulnerability is also known as insecure de-serialization.

A successful attack could lead to PHP creating any object the attacker chooses, with the values the attacker chooses. Depending on the PHP codebase, this could have little effect on the website or could lead to actions being performed within PHP without any security or safety checks.

Fun Fact: While the only officially supported version of WordPress Core is the most recent release, the WordPress core team included backports to address security issues found in 2021 all the way back to WordPress 3.7 "Count Basie", which was originally released in 2013.

Fear of dependency confusion attacks

Dependency confusion is a risk that is caused when a piece of software's auto-updating functionality can be tricked into updating software from the wrong source. For WordPress, dependency confusion attacks put custom plugins at high risk of being updated from the wrong source.

If a custom plugin shares the same name or "slug" as a plugin available via the WordPress.org plugin repository, the auto-update mechanism in WordPress core would have updated with the WordPress.org plugin repository version, but this is no longer the case as of WordPress 5.8.

The WordPress Core team added a feature in 2021 to protect sites from dependency confusion attacks. This new security feature allows developers of plugins to identify the source URI and update method for their plugin(s), ensuring the plugins are being updated from the same originating source.

WordPress.org vulnerability disclosure policy and bug bounty program

Another sign of a mature product is the WordPress.org vulnerability disclosure policy and bug bounty program. All of the reported vulnerabilities in WordPress Core in 2021 were reported through this vulnerability disclosure program which sets forth proper rules and expectations for all parties involved.

Patchstack encourages all developers, including small open-source developers to have a public vulnerability disclosure policy. You do not need to pay big bug bounties to have one, and a vulnerability disclosure policy is exactly where you can state you offer no bounties on security bugs at all.

Public vulnerability disclosure policies are about setting expectations and stating who is responsible for reviewing security reports for the project and how to get in contact with them. Policies that go the extra mile and include bug bounty details are also great, but not required.

03 WordPress themes

Feature-filled themes help users build websites with ease. These features though, sometimes lead to themes becoming more than just design. Many themes include PHP code for additional functionality, and, any code added to a website has the possibility of harboring insecurities.



Theme vulnerabilities are just as critical as plugin vulnerabilities

As theme vulnerabilities can be as critical as plugin vulnerabilities, it’s advised to make sure to find a designer who is familiar with security issues and regularly updates their projects.

Site owners should also monitor their websites' themes for security updates, this is just as important as monitoring the plugins.

Out of the theme vulnerabilities reported in 2021, the most critical would lead to a full site compromise via an arbitrary file upload. Patchstack Alliance member Lenon Leite identified over 50 themes that had security issues in their file upload functionalities throughout 2021.

Critical theme vulnerability count in 2021

| | | |
|---|-----------|--------------------|
| Unauthenticated arbitrary file upload and option deletion | CVSS 10.0 | 10 themes affected |
| Unauthenticated Upload vulnerability leading to Remote Code Execution (RCE) | CVSS 9.8 | 1 theme affected |
| Unauthenticated Blind SQL Injection (SQLi) vulnerability | CVSS 9.8 | 1 theme affected |
| Arbitrary File Upload vulnerability | CVSS 8.8 | 42 theme affected |
| Unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability | CVSS 8.8 | 1 theme affected |

The trend of critical vulnerabilities in themes

2021 showed a continued trend of critical vulnerabilities in themes related to file upload features provided by the WordPress theme. This is not a new trend, but a recurring issue related to the fact that themes commonly include custom code for file upload functionality.

File upload vulnerabilities are critical to websites. These sorts of vulnerabilities are sought after by attackers, because being able to upload a web shell in a PHP file, is basically the same as a full site compromise.


WebHosts or Advanced users may want to consider disallowing the execution of PHP files in the file upload directories. This can be done via Apache .htaccess file, Nginx rules, or even a WAF firewall rule.

Simply block access to URLs ending in “.php” with URLs that contain the word “upload” (or match your known upload paths). This is a relatively sane protection to implement, as website uploads are intended to be media like images, videos, or pdfs, but not PHP code.

04 WordPress plugins


In 2021 there were **35 critical vulnerabilities** reported in WordPress plugins. Two of these critical vulnerabilities were found in plugins with over one million installations. These likely had many users scrambling to update their sites and hosting providers rushing to apply firewall rules to protect their customers.

The two plugins with over 1 million installations addressed critical vulnerabilities in 2021:



All in One SEO plugin <= 4.1.5.2
Authenticated Privilege Escalation vulnerability

3+ million

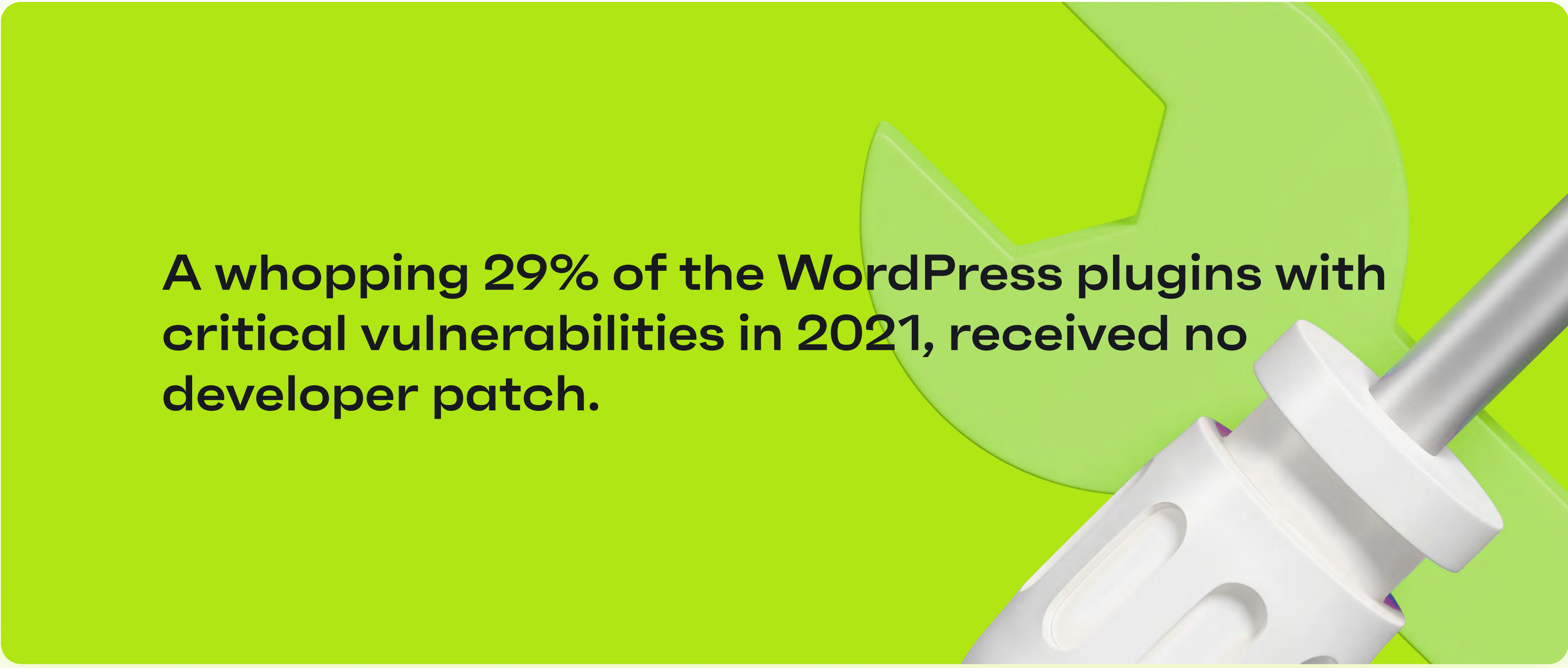


WP Fastest Cache plugin <=0.0.4
Cross-Site Request Forgery (CSRF) leading to Stored Cross-Site Scripting (XSS)

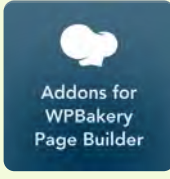
1+ million

We applaud the developers of these plugins for taking responsibility and acting quickly to get a security patch released. These vulnerabilities are on the lighter side of critical, as they had per-requisites such as a valid user account or interaction with a user on the site, but either could have resulted in significant impact if an attacker was successful in their attack.

The positive action of these two projects is juxtaposed by the inaction by nine projects which had critical vulnerabilities identified in the plugins and with no security patch made available. We will discuss this next.




For example, the following 9 plugins have all been removed from their respective repositories due to not addressing security bugs. Two of the plugins were removed from the Code Canyon marketplace, while the other 7 were removed from the WordPress.org repository.




Modern WPBakery Page Builder Addons Unauthenticated File Upload


Premium




N5 Upload Form plugin Unauthenticated File Upload




WP-Curriculo Vitae Free plugin Unauthenticated File Upload



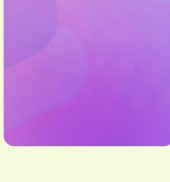
Imagements Unauthenticated File Upload




Business Hours Pro Unauthenticated File Upload



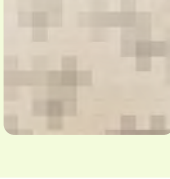
Gallery from files Unauthenticated Remote Code Execution



TheCartPress Privilege Escalation



Car Seller – Auto Classifieds Script Unauthenticated SQL injection



Store Locator Plus Privilege Escalation

Instantly identify new and known vulnerabilities in your WordPress plugins, themes and core.

Check for free >

In these cases where no patches are made available, users need to manually check if they have these plugins installed and remove them or find alternatives. There is no method of communicating this issue directly to website owners running these plugins as the plugins will appear “up to date” in the WordPress administration pages if installed.

Because the insecure components have been removed from their respective repositories, no method to apply a patch is available to site owners running these plugins. In fact, no notice or warning is made available of the risk in running these plugins unless site owners have a security tool like the Patchstack plugin to notify them of insecure components on their websites.

Authorization Checks (or securing AJAX endpoints)

What many of these critical vulnerabilities have in common is the lack of verifying that the user has the appropriate privileges. Most of these vulnerabilities would not exist if this validation was present in the code. In addition, close attention must be paid to:

- **nopriv** endpoints should never perform dangerous actions and should be under high scrutiny
- Use **current_user_can** and **wp_verify_nonce** for privileged endpoints

05 150% rise in vulnerabilities found compared to 2020

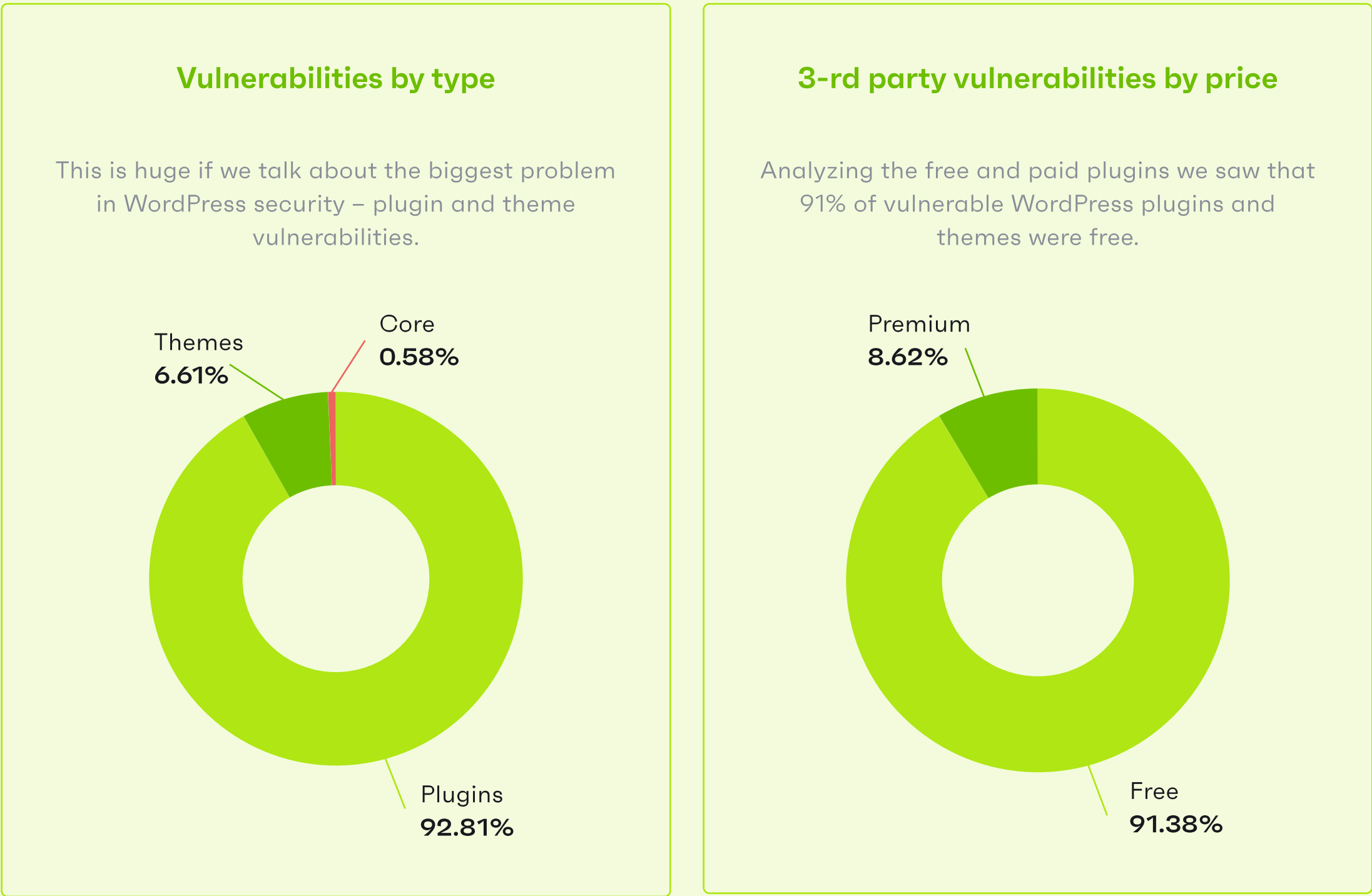
In 2021, Patchstack added nearly **1500 new vulnerabilities** to the Patchstack database. These vulnerabilities were in WordPress plugins, themes, and WordPress core.

If you compare these numbers with 2020 where we saw nearly 600 new vulnerabilities, it's clear that 2021 has been an exceptional year for the security of the WordPress ecosystem.

The WordPress.org repository leads the way as the primary source for WordPress plugins and themes. Vulnerabilities in these components represented 91.79% of vulnerabilities added to the Patchstack database.

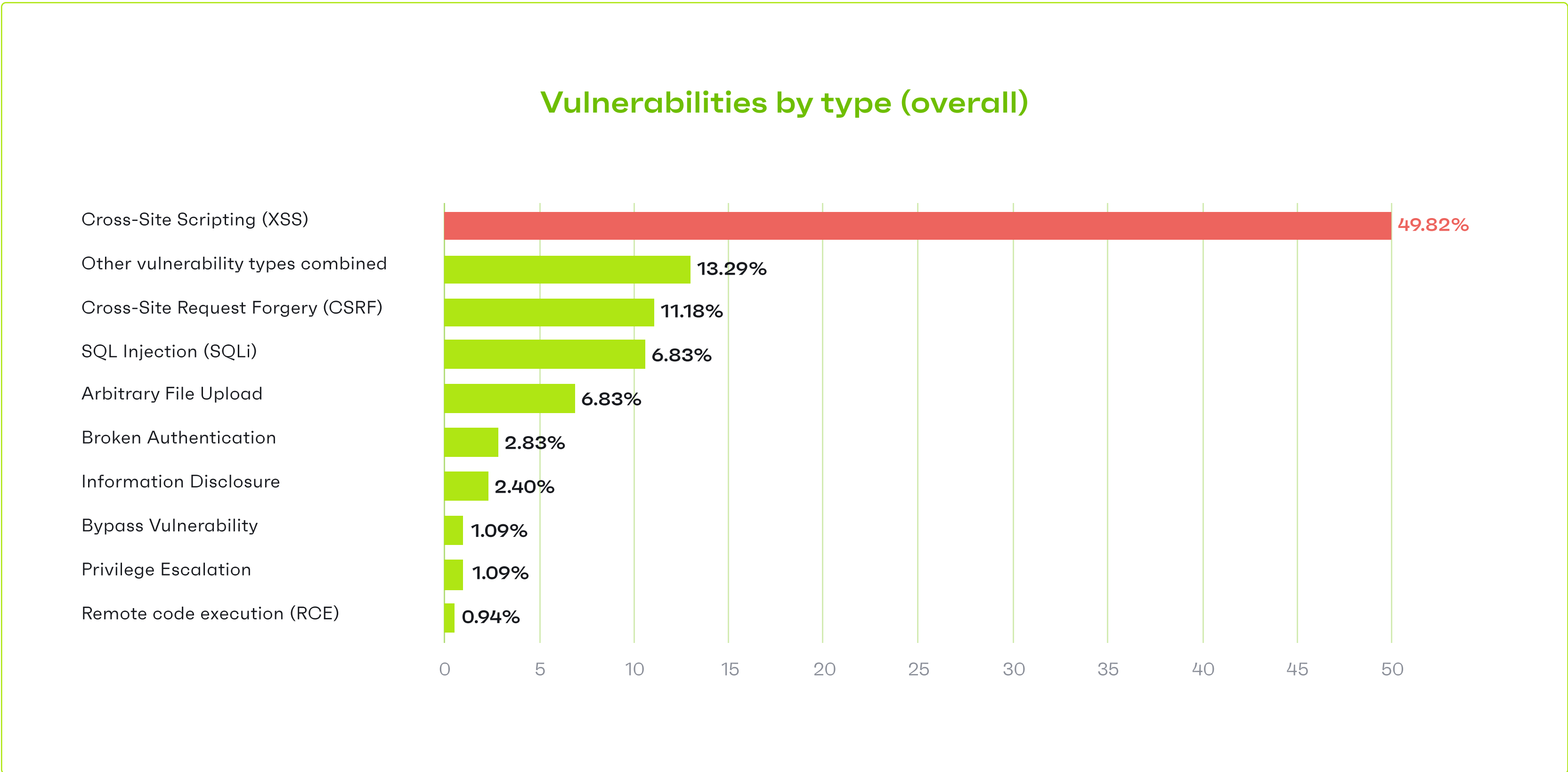
The remaining 8.21% of the reported vulnerabilities in 2021 were reported in premium or paid versions of the WordPress plugins or themes that are sold through other marketplaces like Envato, ThemeForest, Code Canyon, or made available for direct download only.

In 2020 we found 96.22% of vulnerabilities originate from plugins and themes. In 2021 we see that number rise to 99.42%.

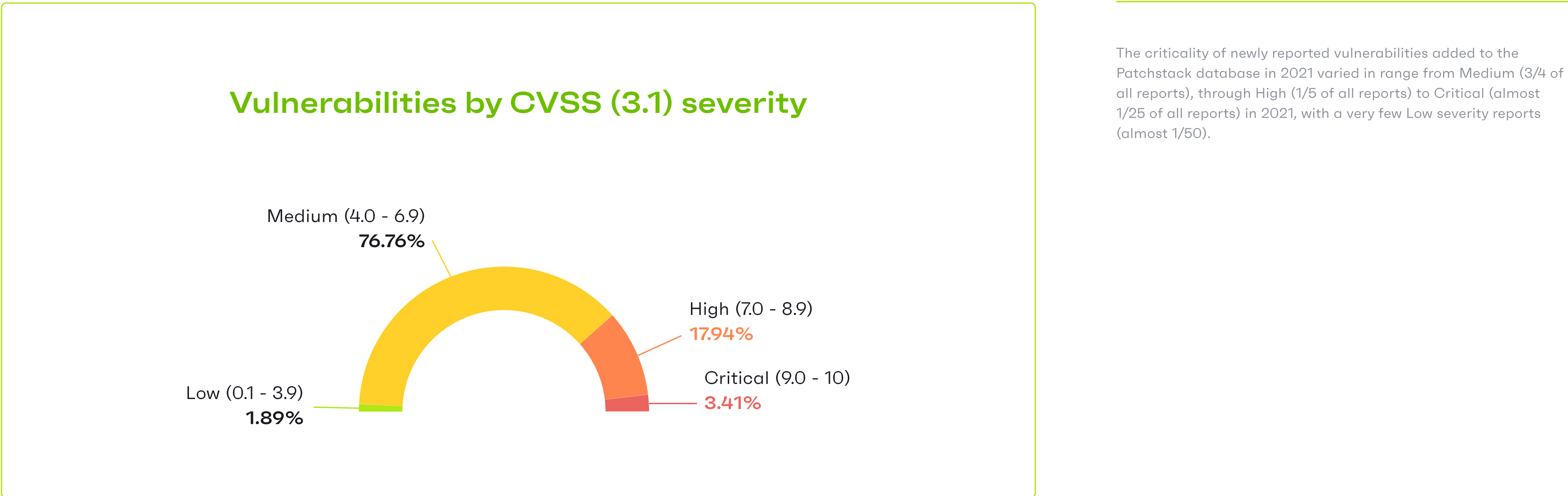


Cross-Site Scripting (XSS) Highly Prevalent

Cross-site scripting (XSS) vulnerabilities once again topped the charts in 2021 accounting for almost 50% of the total vulnerabilities added to the Patchstack Database in 2021. Compared to 2020 – XSS vulnerabilities accounted for a bit more than 36%, in 2021 we see a rise in cross-site scripting vulnerabilities.



When comparing 2020 and 2021 we see CSRF and SQLi have changed places. SQL Injection counted for 9.1% of the vulnerabilities in 2020 and Cross-Site Request Forgery came third with 6.5% of vulnerabilities in 2020.



CVSS (3.1) is a great way to calculate the severity of the vulnerability and it's easier to show the level of risk posed by the vulnerability without writing a broad explanation. That's why we try to calculate CVSS (3.1) score for all vulnerabilities that we're publishing on the database.

You will see a CVSS score with every vulnerability recorded in the Patchstack database. When possible, we also try to add further application-specific context. For example: with WordPress components, we clarify which default user roles would be needed to perform the attack, something CVSS does not cover.

This information shows up as a statement like "Requires subscriber or higher role user authentication." on the vulnerability description page.

It is important to understand the context of a vulnerability's risk. Without that, you could end up needlessly stressing out and performing emergency updates when risk is simply not present, or worse yet, ignoring or delaying addressing a vulnerability because it seems "medium risk" when in fact your websites are at immediate risk based on the context.

06 Fewer plugins are used while more of them are outdated

Patchstack has been offering protection for WordPress sites for years. Looking into Patchstack users we see important information about how our users manage security.

In 2021 we analyzed about 50 000 sites and looked at the installation count of plugins and themes. We found that on average a single WordPress website has **18 different components** (plugins and themes) installed.

Comparing it to 2020 where we found that an average website had 23 plugins and themes installed on a single site. It shows improvement until we compare the number of average outdated plugins and themes on a site.



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

Find out about vulnerabilities in your WordPress websites!

[Sign up for free >](#)

In 2020 we saw 4 out of 23 components outdated and **in 2021 we saw 6 out of 18 components outdated** on a single WordPress site. With every additional plugin installed on the website, the risk of being exposed to a potential vulnerability increases. The fact that websites are lagging behind with updates increases the risk even more.

07 Easy to exploit vulnerabilities remain the main targets

Typically, only easy to exploit vulnerabilities are targeted. Vulnerabilities that have more prerequisites for successful exploitation are mostly not used in mass exploitation campaigns.

Vulnerabilities that we see being weaponized in mass exploitation campaigns don't require any authentication. Below is a list of vulnerability types that are most attractive to the attackers.



Unauthenticated stored cross-site scripting that affects the frontend

Such vulnerabilities make it possible to inject HTML, or in many cases a JavaScript file of a third-party malicious site, that will redirect users to a different site or inject advertisements.



Unauthenticated privilege escalation

Such vulnerabilities make it possible to create an administrator account as a guest. After this, an attacker will log in to this administrator account and upload a malicious plugin that allows them to get access to the filesystem of the site so they can more easily upload backdoors and inject advertisements.



Unauthenticated options update

Such vulnerabilities make it possible to turn on registrations and set the default role to administrator. It also makes it possible to change the URL of the site to something else so all visitors get redirected to this malicious URL.



Unauthenticated remote code execution

Being able to execute code, such as any arbitrary PHP code, is also ideal for a malicious user to exploit. They can upload a backdoor this way to easily gain access to the filesystem of the website.

These types of vulnerabilities, especially the ones in popular plugins are often exploited within hours of the vulnerability being disclosed to the public.

08 Old vulnerabilities remain targeted

When looking at the statistics of Patchstack virtual patches to see which vulnerabilities were most actively targeted, some critical vulnerabilities that date back years are still being actively exploited.

This can be explained as the use of “hacking tools” that are available online. Such tools are pre-programmed to attempt all exploits and popular vulnerabilities against a target, and all the hacker needs to do is select a target website (or list of targets.)

Below is a list of top vulnerabilities that are being attacked the most on a daily basis.

Top 4 attacked vulnerabilities (from 2021)



OptinMonster <= 2.6.4
Unprotected REST-API to Sensitive Information Disclosure and Unauthorized API access



PublishPress Capabilities <= 2.3
Unauthenticated Settings Change vulnerability

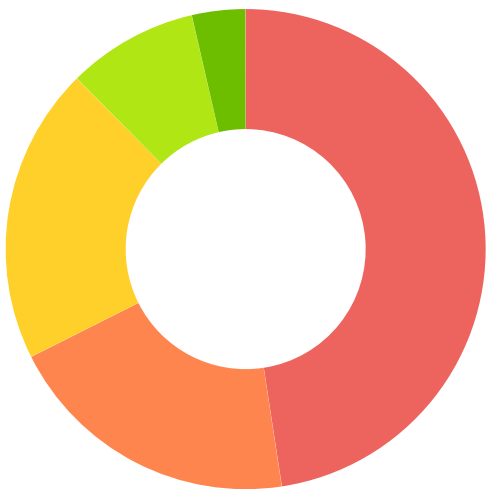


Booster for WooCommerce plugin <= 5.4.3
Authentication Bypass vulnerability



Image Hover Effects Ultimate plugin <= 9.6.1
Unauthenticated Arbitrary Options Update

Most targeted plugins (all time)



- WordPress Social Warfare: **47.6%**
- Duplicator: **20%**
- ThemeRex Addons: **20%**
- All in One SEO: **8.8%**
- All other plugins: **3.6%**

09 \$12,850 to ethical hackers for securing plugins

Patchstack Alliance is a bug hunting platform that connects ethical hackers with open-source vendors to improve the security of the open-source web. Patchstack Alliance has members from Germany, France, Russia, Portugal, Brazil, Vietnam, Columbia, Netherlands, India, Estonia, Lithuania, Myanmar, Thailand, Malaysia, China, Indonesia.

In 2021 Patchstack paid **12,850.00 USD** in bounties. Since April 2021, we received more than 1000 vulnerability reports from the Alliance members.

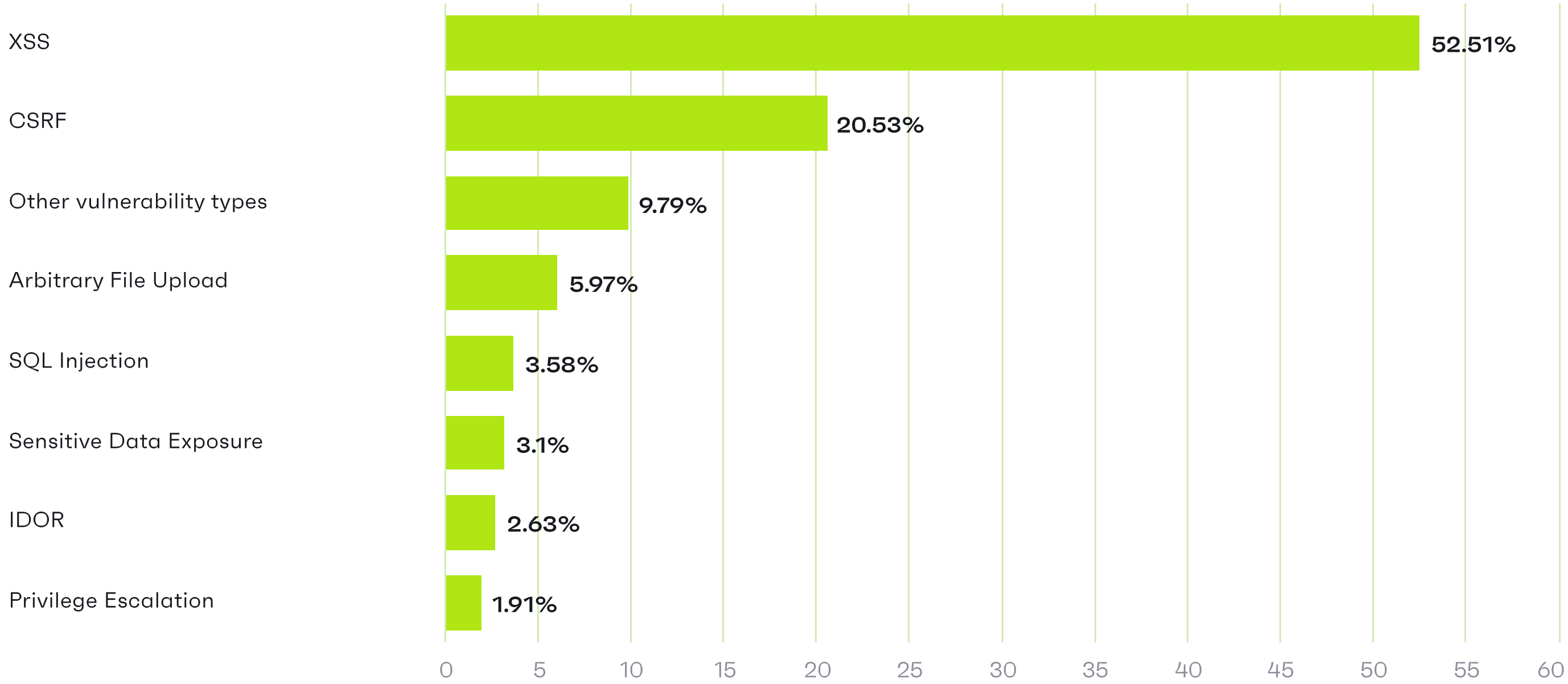
The biggest count of vulnerable points/parameters found in a single plugin was 47. We’ve accepted reports that affected plugins with less than ten active installs and also ones with over 5 million active installations. The most popular vulnerabilities reported by the members of Patchstack Alliance are XSS and CSRF.

The first year has proven a strong interest in the program by ethical hackers, open-source vendors, and also partners such as hosting companies.

Be first to know about new vulnerabilities with Patchstack Threat Intel Feed (API)

Read more >

Most popular vulnerabilities reported to Patchstack Alliance bug bounty program



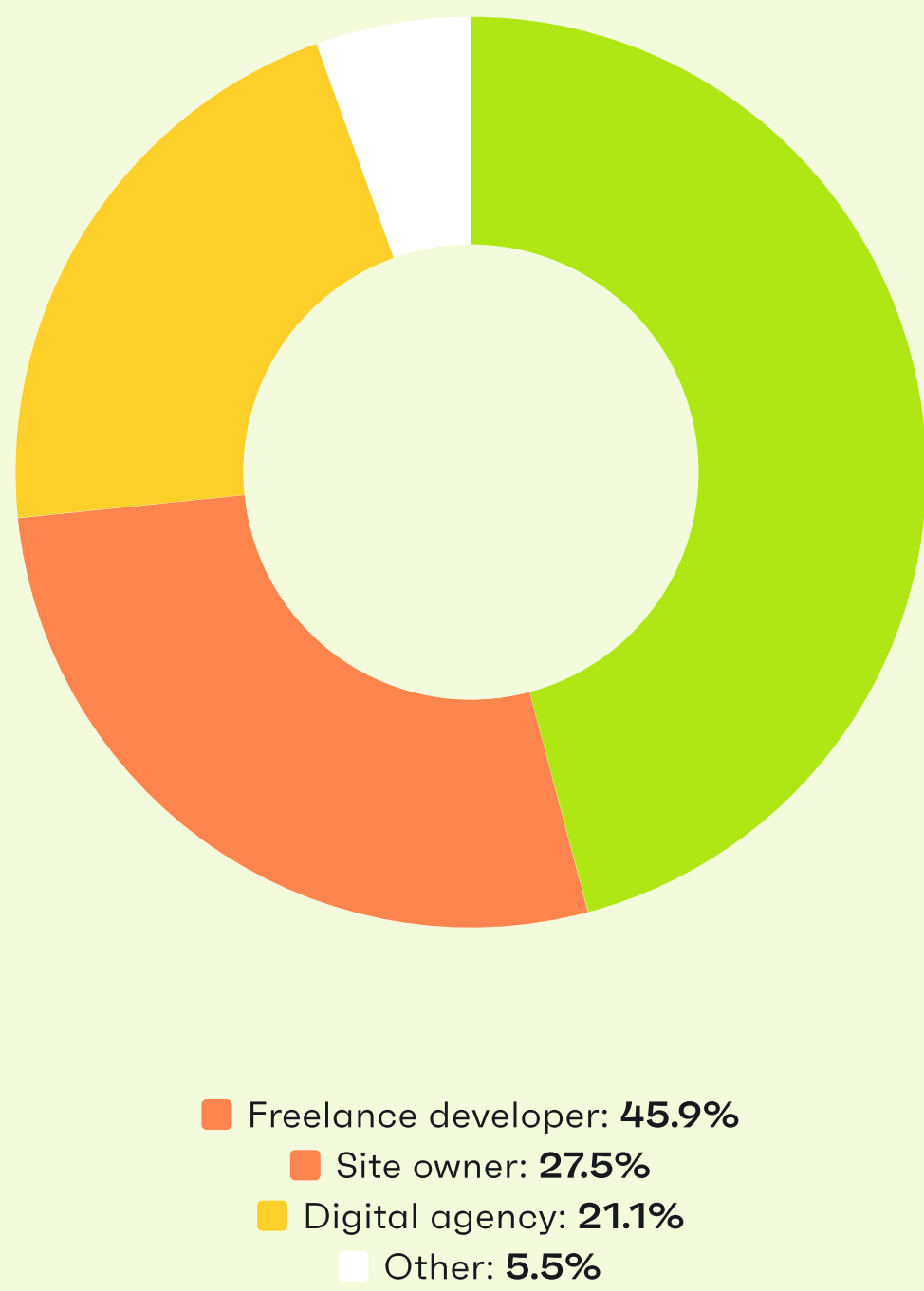
i If you’d like to get involved or would like to support the initiative, please reach out to us.

Learn more >

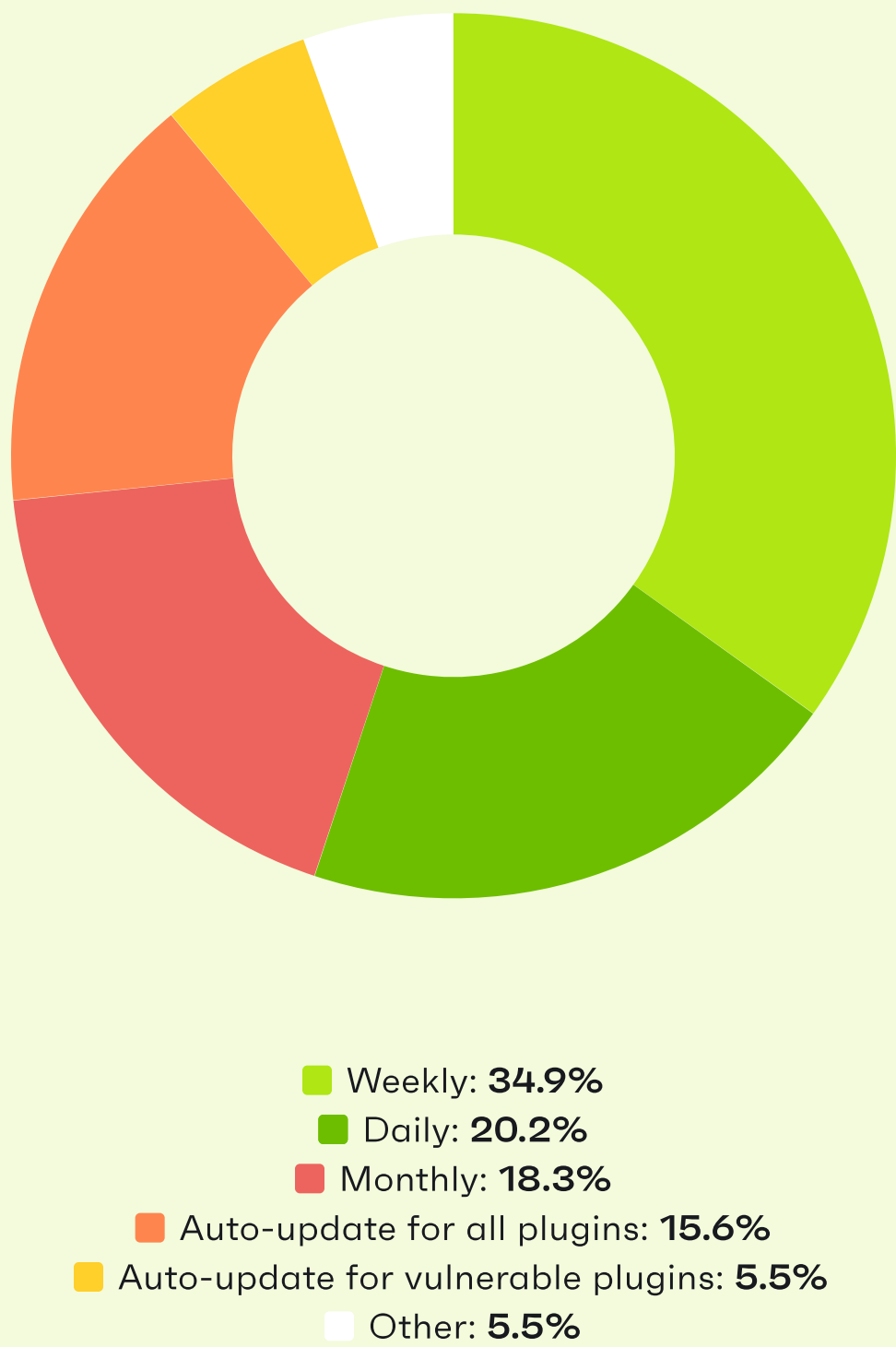
10 Increased awareness around vulnerabilities

During the end of 2021 Patchstack **conducted a survey** among website developers, website owners, and digital agencies. The aim of the survey was to get an understanding of how was the year 2021 regarding WordPress security.

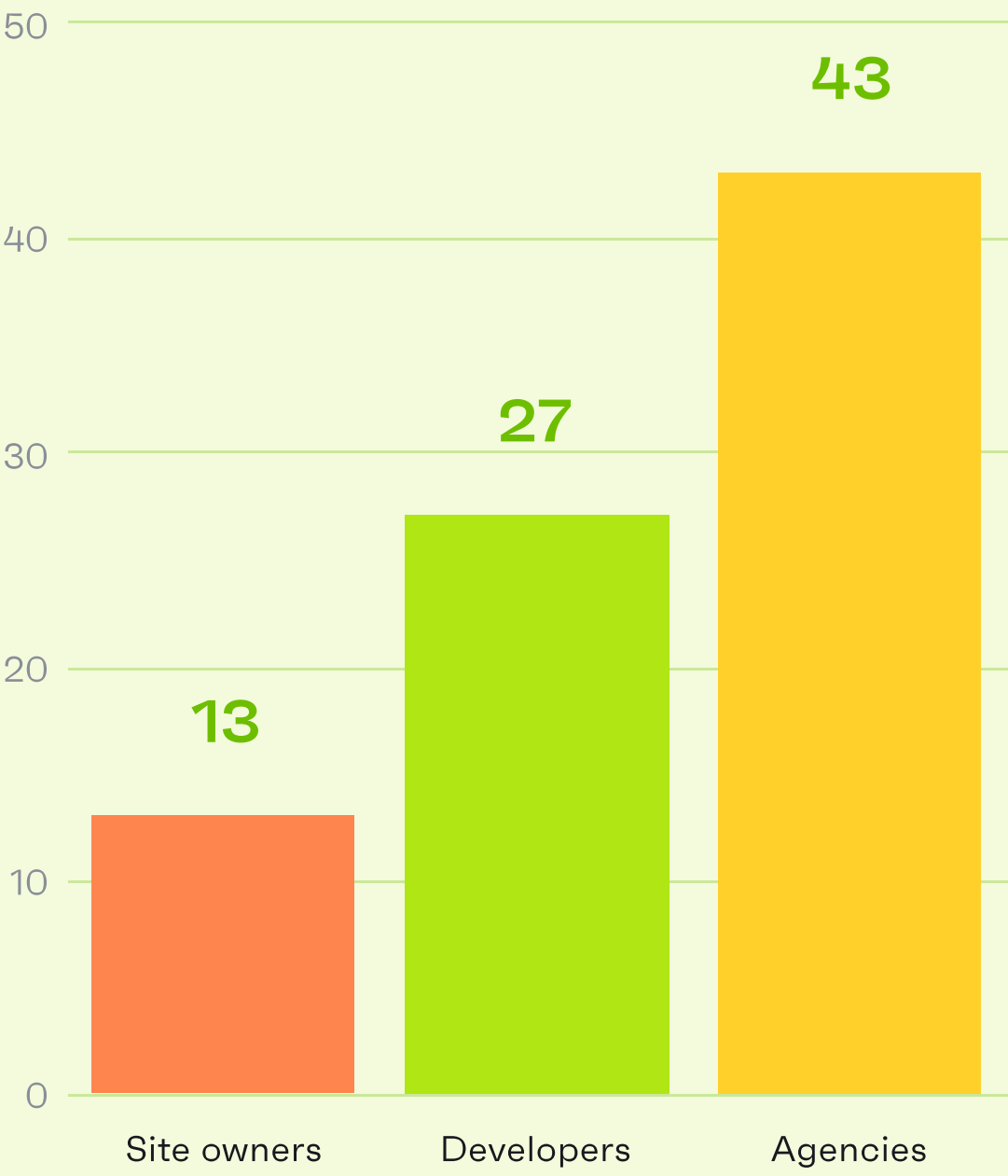
Describe your role



Updating frequency



Average #no of websites



Save time and money by enabling auto-updates for vulnerable plugins and themes with Patchstack.

[See all features >](#)

When asking the respondents who they rely on for website security help, the majority said they deal with security issues primarily by themselves, while also relying on their hosting provider or a security plugin's support team.

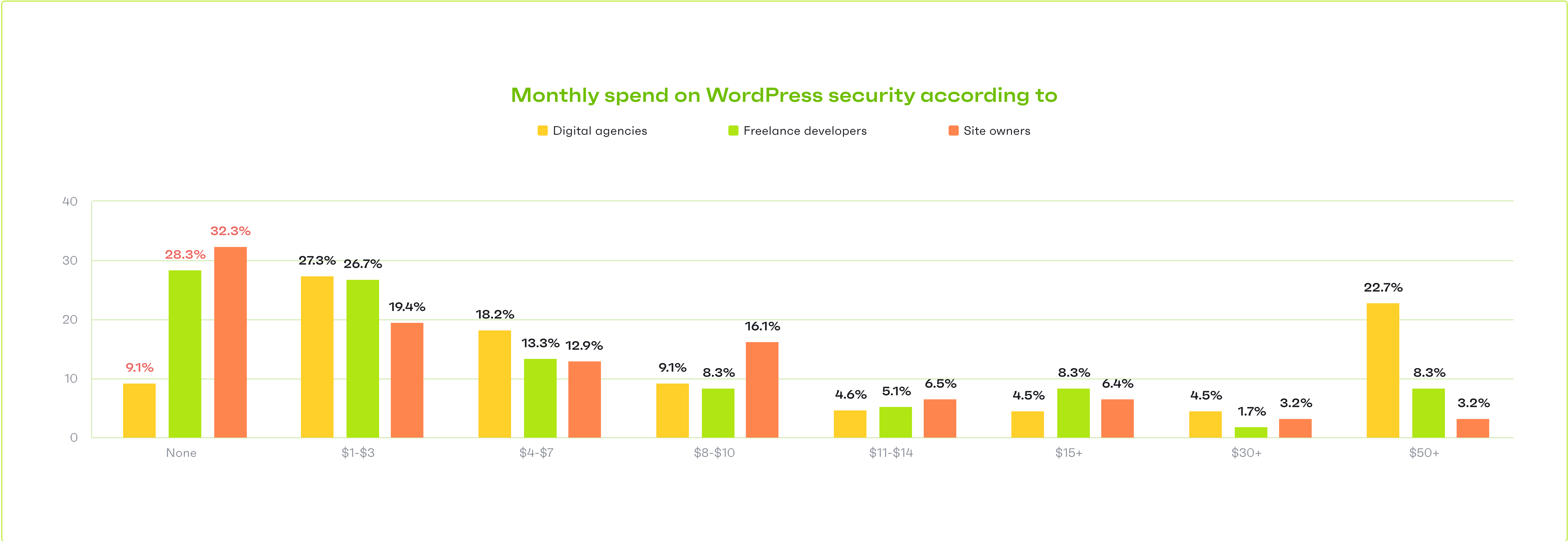
In WordPress security updates are a very important task of vulnerability management. We asked the respondents how often they update their plugins, themes, and WordPress core. Around 53% of the respondents stated they update their components weekly. 20% of respondents stated they perform updates daily and 18% monthly. Others have auto-updated enabled or have no information due to not being responsible for updates.

11 Website security budgets are almost nonexistent

The WordPress ecosystem has countless security plugins and tools to choose from. Some of the tools are free, some cost up to hundreds per month. We wanted to know what is the average spend on website security among website owners, developers, and digital agencies.

Based on the data we gathered **28%** of the respondents had **zero budget** to protect their websites. About 27% of the respondents stated their website's security budget per website per month is between 1-3 dollars.

Only about 7% of the respondents said their website security budget is around \$50 per site per month and most of these respondents were from digital agencies.



The average cost for WordPress malware removal in 2021 was \$613.

Save time and money by protecting websites from the #1 reason they get hacked.

Start your free trial >

When looking at costs for malware removal we saw that the respondents spend on average \$613 for a WordPress malware removal. The highest price paid was \$4,800 and the lowest was \$50.

The average cost for website security among those who got their websites hacked during 2021 was around \$8 per site/per month.

The biggest problem in WordPress security remains

For the second year in the row (see 2020 survey report here), we have found that respondents see that the biggest problem in WordPress security is - WordPress core, plugin, and theme vulnerabilities.

The most popular challenges faced when dealing with website security in 2020 were lack of knowledge, blocking and preventing attacks, and plugin and theme vulnerabilities.

In 2021 the challenges remain the same. More than half of the respondents (59%) responded that in their opinion **the biggest problem in WordPress security is core, plugin, and theme vulnerabilities**.

About 15% shared that in their opinion insecure passwords are the biggest problem in WordPress security. The same amount of respondents said the biggest problem is nulled (malicious) plugins, themes. A little more than 9% of the respondents saw the biggest problem to be an insecure hosting environment.

It's probably no surprise that people use bad passwords. A study of publicly-available "hacked" accounts reveals '123456' was the top used password, followed by '123456789' and 'qwerty'.

12 Conclusion

Vulnerabilities from plugins and themes remain as one of the biggest threats to websites built on WordPress. In fact, 99.42% of security vulnerabilities were found in WordPress plugins and themes, while only 0.58% of security vulnerabilities originated from WordPress Core.

We've seen a 150% growth in vulnerabilities reported in 2021 compared to 2020 which is a significant increase. Meanwhile, 29% of the WordPress plugins with critical vulnerabilities received no patch.

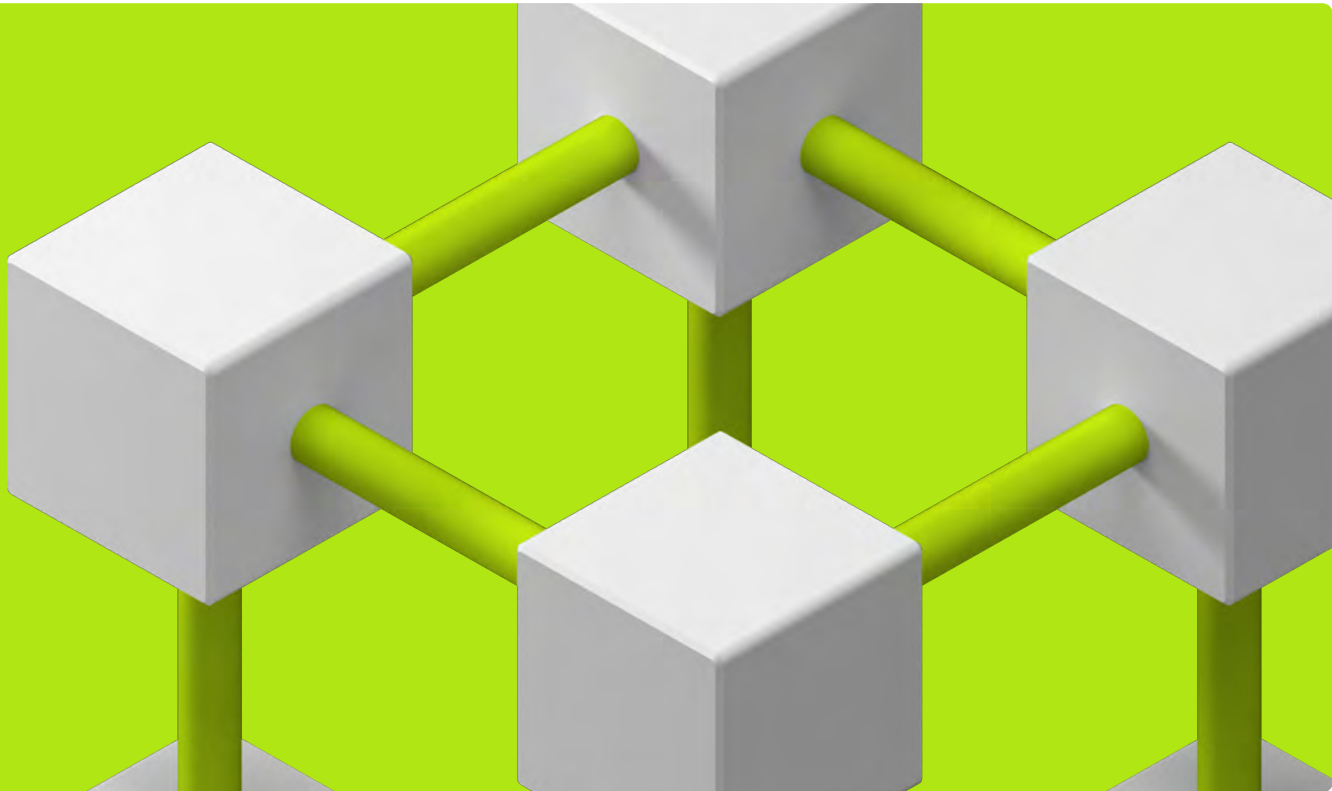
In 2021, Patchstack launched a bug bounty community for ethical hackers (Patchstack Alliance) to identify and patch vulnerabilities across the entire WordPress ecosystem. In 2021, around \$13,000 was paid out as bounties. Brands such as Plesk, cPanel, Pagely, and many others are already supporting it. [Support the movement!](#)

Sources

<https://patchstack.com/database/?search=&type=core>
https://codex.wordpress.org/Supported_Versions
<https://patchstack.com/database/vulnerability/wordpress/wordpress-5-7-object-injection-in-phpmailer-vulnerability-cve-2020-36326>
<https://patchstack.com/database/vulnerability/wordpress/wordpress-core-5-8-command-injection-vulnerability-in-the-lodash-library>
<https://patchstack.com/database/vulnerability/wordpress/wordpress-core-5-8-1-expired-dst-root-ca-x3-certificate-issue>
<https://patchstack.com/database/vulnerability/wordpress/wordpress-5-7-4-plugin-confusion-vulnerability>
<https://patchstack.com/patchstack-weekly-week-48-dependency-confusion/>
<https://make.wordpress.org/core/2021/06/29/introducing-update-uri-plugin-header-in-wordpress-5-8/>
<https://patchstack.com/wp-content/uploads/2021/04/Security-vulnerabilities-of-WordPress-ecosystem-in-2020-Patchstack-1.pdf>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36845>
<https://patchstack.com/articles/patchstack-cve-numbering-authority/>
https://w3techs.com/technologies/history_overview/content_management/all/y

**Protect your WordPress websites with
our limited offer -50% off.**

Check pricing and features >



13 Further reading and listening



Hackuu



Follow Hackuu – a hero who helps security researchers share vulnerability info and secure the WordPress ecosystem.

[Follow on Twitter >](#)

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 >](#)



Identify and patch plugin, theme and core vulnerabilities in your WordPress sites