patchstack

Security vulnerabilities of WordPress ecosystem in 2020

By Oliver Sild, Founder and CEO of Patchstack
April, 2021

Analysis of security vulnerabilities found in WordPress core, plugins and themes in 2020.

Learn more from patchstack.com

WordPress is the most popular content management system in the world. Just recently, it reached a milestone of powering 41% of the websites on the whole web.

Like many other web development frameworks, WordPress is open-source, and anyone can expand its functionality with custom plugins and themes.

Developers and users of WordPress can simply navigate to the WordPress plugins repository if they wish to expand their website's functionality with a third-party extension.

After all, there are more than 58 000 plugins to choose from.

582 security vulnerabilities found in 2020

Just in 2020 alone, the data of the Patchstack Database reveals that 582 unique security vulnerabilities were found in total. These vulnerabilities affected WordPress core and third-party plugins and themes.

The most common vulnerabilities are Cross-Site Scripting which accounts for more than 36.2% of the total unique vulnerabilities found in 2020.

SQL Injection counts for 9.1% of the vulnerabilities and Cross-Site Request Forgery comes third with 6.5% of vulnerabilities.

Top 5 ranking based on vulnerability types

Vulnerability	Unique cases
Cross-Site Scripting (XSS)	211
SQL injection (SQLi)	53
Cross-Site Request Forgery (CSRF)	38
Sensitive Information Disclosure	29
Arbitrary File Upload	16
Other	131

Source: Patchstack Database

Top 5 ranking based on OWASP 10

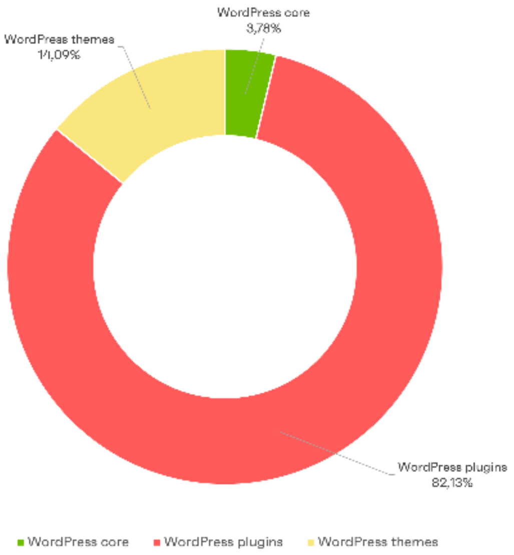
Vulnerability	OWASP ranking	Unique cases
Cross-Site Scripting (XSS)	A7	211
Injection	A1	70
Cross-Site Request Forgery (CSRF)	Not in Top 10, A8 in previous version (2013)	38
Sensitive Data Exposure	A3	29
Other	MISC	130

Source: Patchstack Database

96.22% of vulnerabilities originate from third-party code

Only 22 vulnerabilities in 2020 were found in WordPress core. Every other vulnerability was either found in a third-party plugin or in a theme.

Vulnerabilities on WordPress core, themes and plugins.



Source: Patchstack Database

While 82 unique vulnerabilities were found in WordPress themes **a whopping 478 security issues were found in plugins.**

The vulnerabilities found in plugins and themes tend to be more severe than those found in WordPress core.

What makes matters worse is that many popular plugins have millions of active installations and the numbers aren't pretty when we look at how many websites are affected by the vulnerable plugins.

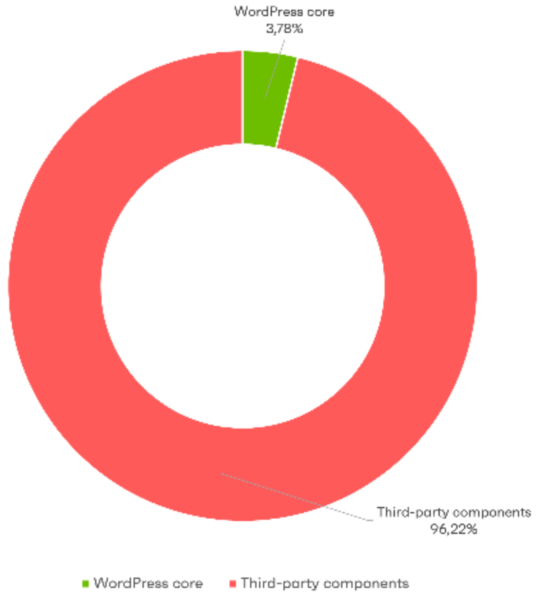
Active installations of vulnerable plugins in Q1 and Q2 of 2020

Month	Unique cases
January 2020	7M
February 2020	400K
March 2020	5M
April 2020	1M
May 2020	12M
June 2020	6M

Source: Patchstack Database

The data above shows the active installation count at the moment when a vulnerability was disclosed in a given plugin.

96.22% of vulnerabilities originate from third-party code.



Source: Patchstack Database

The security vulnerabilities which were found in plugins and themes had a total active installation count of 70 million.

Thats almost as many websites there are build with WordPress. The official WordCamp website claims there are currently 75 million websites powered by WordPress.

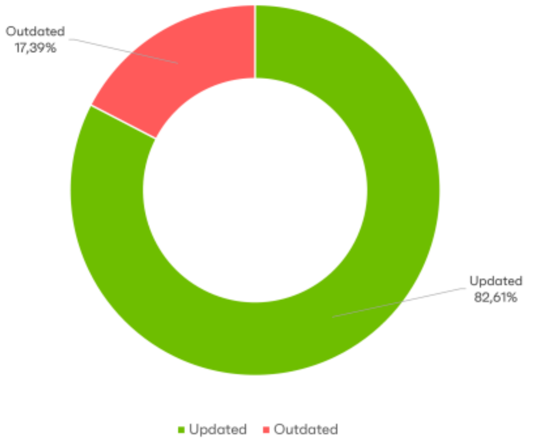
23 third-party plugins per WordPress site

We analyzed 50,000 websites and looked at the installation count of plugins and themes.

We found that on average a single WordPress website has 23 different third-party components installed. Meanwhile, about 4 out of 23 were outdated and had a new version available.

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.

Websites are not updated regularly.



Source: Patchstack Database

Web developers becoming increasingly worried

In the second quarter of 2020, Patchstack surveyed nearly 400 web developers, freelancers, and digital agencies to get their thoughts on website security.

The responses clearly showed that they were well aware of the security challenges WordPress can introduce.

Over 70% responded that they were **increasingly worried about the security of their website** and the top reason was "vulnerabilities in third-party plugins".

About 45% of respondents saw an increase in attacks on websites they were managing and 25% had to deal with a hacked website in the month prior to participating in the survey.

Conclusion

Vulnerabilities from **third-party code remain as one of the biggest threats to websites** build on WordPress.

We already see a growth in unique vulnerabilities reported in the WordPress plugins and themes comparing 2020 with the beginning of 2021.

Different security companies in the WordPress ecosystem have already done a great job to provide numerous solutions to provide remediation to the attacks and malware infections.

Patchstack has created a free vulnerability database to find the latest vulnerabilities affecting WordPress applications.

Patchstack has also started an initiative to build a community of independent security researchers (Patchstack Red Team) behind the WordPress ecosystem through a gamified bug bounty platform.

All web hosting companies and other vendors providing services to the WordPress ecosystem are invited to support the initiative.

We at Patchstack believe that now it's time to seriously address the core issue. Third-party code needs better auditing this requires a community effort!

Patchstack is an Estonian cybersecurity company. It allows more than 50,000 developers to detect and patch third-party code vulnerabilities. The company was accelerated by the Cylon cybersecurity startup accelerator in London and has won numerous startup competitions such as Salto Growth Camp.

Oliver Sild, Founder & CEO of Patchstack
Contact via **oliver.sild@patchstack.com**
www.patchstack.com