WORDPRESS PLUGINS COULD LEAVE ONLINE SHOPPERS & BUSINESSES VULNERABLE ON CYBER MONDAY

As American shoppers gear up for the biggest shopping weekend of the year - the perfect storm of Thanksgiving Day, Black Friday and Cyber Monday- more and more shoppers are preparing to do their purchasing online from the comfort of their homes.

Winning the battle of the holiday bucks in 2015 was Cyber Monday where shoppers spent $3.07 billion of which $799 million, 26% of the total sales, were made from mobile devices.

2015 Shopping Comparison: Thanksgiving Day $1.73 billion; Black Friday $2.74 billion; Cyber Monday $3.07 billion.

While racing to be first in line for the best deals in shopping malls and traditional brick and mortar retail stores can result in injury, switching your shopping strategy from offline to online for the triple crown of capitalism doesn't come without its own risks.

In 2015, email marketing was a major driver of traffic for the holiday weekend with emails driving over 22% of Cyber Monday orders. Mobile purchasing increased 23% from 2014 to 2015 with shoppers making 27% of their purchases with their mobile devices, a trend set to reach even higher heights here in 2016.

As the revenue generated from these "high holidays" of shopping continues to soar, it's critical that shoppers are aware and alert as the potential threats which could be lurking behind the platforms and websites where they are conducting their transactions.

WORDPRESS PLUGINS AND THE POTENTIAL DANGERS LURKING WITHIN

With well over a million websites using various e-commerce content management system (CMS) plugins to power the purchases that they offer, our research has made it clear that some are less secure than many would expect.

The security state of WordPress plugins made major headlines in April when the largest data leak in history, the "Panama Papers," was revealed. The victim, Mossack-Fonseca, was a key player in the shadowy world of shell companies and offshore accounts, however despite their relentless efforts to protect the secrets of their clients, they had over 2.5 terabytes of data accessed and leaked in part due to their lapsed security when it came to their content management systems (CMS).

When it came to the unraveling of Mossack-Fonseca, the culprit was an out-of-date version of a WordPress image slider plugin that contained a vulnerability that, according to the CEO of the company behind the popular WordPress security plugin WordFence, contained a weakness that was, “trivially easy to exploit.”

As over 26% of all websites globally use WordPress as their platform, up from 18% in 2013, developers, web administrators and users should be cautious when building, browsing and shopping.

Given WordPress’ ease of use and growing market share, it’s no surprise that its platform, plugins and websites are a common target for attacks.

Vulnerabilities contained within plugins can easily, and quickly, infect millions of websites as was the case with the 2011 TimThumb LFI vulnerability which affected 1.2 million websites and caused the redirection of 200,000 WordPress based pages to rogue sites.

Examining the Security Posture of the Top WordPress e-Commerce Plugins in 2016
In order to gain a better understanding of the potential threats posed by the hundreds of thousands of websites which utilize e-commerce plugins, the Checkmarx research lab used CxSAST, Checkmarx’s static code analysis solution to run a scan of the most used WordPress e-commerce plugins in the weeks leading up to Cyber Monday.

Research Summary (Initial Brief)
A more detailed research summary will be available in the future.

Our research focused specifically on scanning for high-level vulnerabilities and 12 WordPress e-commerce plugins were scanned during our research which was conducted throughout the first half of November 2016. The security state of the plugins that were scanned is alarming, however due to the fact that we want to ensure that the organizations behind these plugins have enough time to remediate the found vulnerabilities, the specifics will be anonymous to keep our findings in-line with responsible disclosure.

Out of the 12 plugins we are scanning we have detected high-risk vulnerabilities in at least four of them. One plugin contained three vulnerabilities while the other three each contained one.

Of the found vulnerabilities so far, Reflected XSS was found on three plugins, an SQL injection was found on one plugin, Second Order SQL Injection found on one plugin with File Manipulation also being detected on one plugin.

Of the vulnerabilities that we have detected so far, if they were exploited, the users of over 135,000 websites could find their personal data threatened by malicious parties or cyber criminals.

While most of these plugins are updated regularly, we are unable to comment on if there are patched versions until we notify the organizations behind the plugins about the possibility of having an open attack vector.

HIGH-RISK VULNERABILITIES FOUND IN THE TOP E-COMMERCE PLUGINS:

REFLECTED XSS

What is it:
Using social engineering, an attacker could cause a user to send the website engineered input, rewriting web pages and inserting malicious scripts.

Potential Impact on Business:
Once exploited, the attacker can then pretend to be the original website, which would enable them to steal the user's password, request the user's credit card information, provide false information, or run malware. From the victim's point of view, this is the original website, and the victim would blame the site for incurred damage.

SQL INJECTION (SQLI)

What is it:
Generally speaking, SQL injections are unsanitized user input vulnerabilities. The most common exploitation is in log-in fields of unprotected web and mobile applications. Since all modern applications (web and mobile) use centralized databases to deliver and render information, such hacking opportunities exist in virtually all leading e-commerce, social and financial websites and applications.

Potential Impact on Business:
The damage that can occur when an SQL injection is exploited includes the stealing of usernames and passwords for commercial or criminal purposes, a complete wiping out of content or defacing of website pages (i.e hacktivism), silent spying and/or monitoring of information by competitors.
In extreme cases, the exploit could result in the corruption, and destruction, of entire databases as well as a complete remote takeover of the server.

SECOND ORDER SQL INJECTION (SQLI)

What is it:
Applications communicate with their database by sending a textual SQL query. The application creates the query by simply concatenating strings including data obtained from the database. Since that data may have been previously obtained from user input, and is neither checked for data type validity nor subsequently sanitized, the data could contain SQL commands that would be interpreted as such by the database.

Potential Impact on Business:
With a second order SQLi vulnerability, an attacker could directly access all of the system's data. The attacker would be able to steal any sensitive information stored by the system (such as personal user details or credit cards), and possibly change or erase existing data.

FILE MANIPULATION

What is it:
File manipulation vulnerabilities occur when files, or directories are able to be manipulated in ways that the developer did not intend them to be, thus giving the user, or malicious party, access to modify either the file or directory which could lead to devastating consequences from either the plugin other users.

Potential Impact on Business:
Cyber criminals could exploit a file manipulation vulnerabilities contained within a shopping cart plugin and adjust the files to change the prices during the checkout stage of processing.

TIPS FOR BUSINESSES WORKING WITH WORDPRESS PLUGINS

When it comes to security issues facing WordPress plugins, in addition to the end user, businesses using WordPress e-commerce plugins take certain steps to avoid introducing risks into their websites.

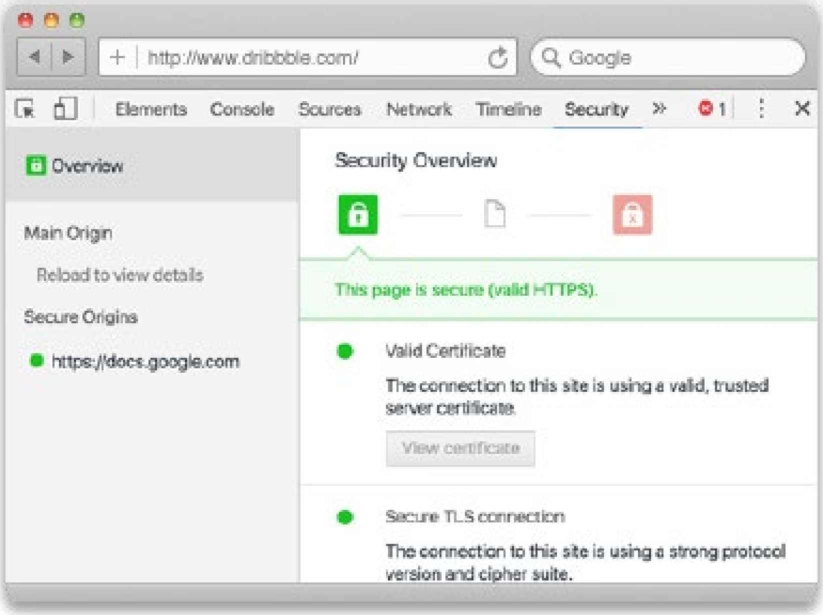
Regardless of the size of your business, it's critical to only download plugins from trusted sources, and in this case WordPress.org should be the only place where you download plugins as the ease of which WordPress plugins are developed makes nefarious plugins a favorite for hackers.

Since WordPress plugins are open-source, it's possible to scan the source code with a static source code analysis solution in order to ensure that it is vulnerability free. It's also important to ensure that all plugins stay up to date and to stay on top of any WordPress vulnerabilities through the WordPress Vulnerability Database.

TIPS FOR CYBER MONDAY SHOPPERS:

If you're planning to shop up a storm this Cyber Monday, there are a few precautions that you can to make your user details harder to hack. This may be obvious, but avoid using simple passwords and never use passwords on more than one site or platform. When possible enable two-factor authentication to further fortify your private user data.

When you're checking in to see what deals a website offers, or when you're ready to check out, be sure to double check the validity of the SSL Certificate. If there is an "S" in the "http" prefix to the website's URL, Chrome users will be able to click the green lock in order to view the certificate and double check that it is verified.



Security Overview

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a valid, trusted server certificate.

Secure TLS connection

The connection to this site is using a strong protocol version and cipher suite.

(Example of the security overview displayed when clicking a website's SSL Certificate)

Lastly, and perhaps, most importantly, use common sense while shopping. If the deals that pop-up on your social media feed, or land in your inbox, seem too good to be true, they probably are. Simply clicking on an unassuming malicious phishing link could lead to disastrous consequences depending on the situation. According to Verizon's 2016 Data Breach Investigations Report (DBIR), phishing attacks are on the rise with 30% of phishing emails open and 12% of the recipients clicking through to either a risky link or attachment. Be aware, stay alert and shop smart.

ABOUT CHECKMARX

Checkmarx is an Application Security software company, whose mission is to provide enterprise organizations with application security testing products and services that empower developers to deliver secure applications. Amongst the company's 1,000 customers are 5 of the world's top 10 software vendors and many Fortune 500 and government organizations, including SAP, Samsung, and Salesforce.com. For more information about Checkmarx, visit http://www.checkmarx.com
or follow us on twitter: @checkmarx