Sri Lanka Institute of Information Technology

IE2062

Web Security

Bug Bounty Report I

Submitted by:

Student Registration Number	Student Name
IT21197550	Nihila Premakanthan

Date of Submission: 28.05.2023

Acknowledgement

I would like to express my special thanks to our mentor Ms. Chethana Liyanapathirana and Dr. Lakmal Rupansighe for their time and efforts she provided throughout the course, and for the Web Security lecture panel for guiding us through this semester and for helping us by giving examples, guidelines, and advice about the project. Your useful advice and suggestions were really helpful to me during the project's completion. In this aspect, I am eternally grateful to you.

Executive Summary

This report aims to provide an overview of the vulnerability identified in a particular domain. The bug bounty platform called Hackerone was used for this purpose.

This report uses different tools to gather information detect vulnerabilities and perform penetration testing. The tool name Netsparker and Owasp Zap was mainly used to identify the vulnerability. Further this report provides the vulnerability title, vulnerability description, Affected Components, Impact Assessment, Steps to reproduce the vulnerability, proof of concept and the proposed mitigation.

By including these comprehensive details for each vulnerability, the report provides a comprehensive overview of the security weaknesses present within the system and offers actionable insights for remediation and improvement.

Contents

Vulnerability Title

Out-of-date Version (WordPress)

Severity:

Risk Level:
HIGH

Vulnerability Description

An earlier or older version of the WordPress software, a well-known content management system (CMS) used for building and maintaining websites, is referred to as a "out-of-date" version of WordPress. Updates for WordPress are frequently released to enhance functionality, address security flaws, and add new features.

A WordPress version that has been out-of-date indicates that it has not been upgraded to the newest release. This may happen for a number of reasons, including a user's choice to delay or disregard updates or a lack of knowledge on the availability of new versions.

Affected Components

A website's various elements may be impacted by an outdated version of WordPress. The following are the primary factors that may be impacted:

- Security: The biggest worry about using an outdated WordPress version is the potential security flaws it might have. Because they are aware of the flaws in older versions, hackers and other bad guys aggressively target outdated software. By not updating WordPress, you put your website at risk for security breaches, malware infestations, unauthorized access, and other security problems.
- Plugins and Themes: The WordPress core software and numerous third-party developers' plugins and themes are made to function together effortlessly. However, as WordPress develops, it makes changes that necessitate the updating of plugin and theme creators' creations. It's possible that using an outdated WordPress version will cause plugin and theme compatibility problems. They might not work properly, produce mistakes, or even ruin the appearance and operation of the website.

- Performance and Stability: WordPress updates frequently come with performance enhancements, bug fixes, and optimizations. You could lose out on these improvements if you don't upgrade, which could impair the general functionality and stability of your website. The user experience may be negatively impacted by outdated versions' performance bottlenecks, slower loading times, and incompatibility with modern technology, which could perhaps turn visitors away.
- New Features: WordPress upgrades frequently include new features and functionality. These updates improve the CMS's functionality and give website owners more options for personalization, content management, and user interaction. You miss out on these new capabilities if you continue using an outdated version, which limits your capacity to take use of the most recent tools and developments in website construction and maintenance.

Impact Assessment

A website may have a number of effects from using an outdated version of WordPress. An evaluation of the probable effects is provided below:

- Security Vulnerabilities: They are exposed on your website while using an outdated WordPress version. Because they are aware of the flaws in older versions, hackers aggressively target outdated software. Exploiting these vulnerabilities might result in unwanted activity that harms your website and compromises user data, such as defacement, malware infections, unauthorized access, and data breaches.
- Increased Hacking Risk: Hackers who take advantage of known vulnerabilities to gain unauthorized access to websites frequently target outdated WordPress versions. Once they have access, hackers can alter your website, inject dangerous code, put in backdoors, or use it to spread spam or malware. This could harm your reputation, interfere with your internet presence, and possibly result in monetary loss or legal problems.
- Compatibility Problems: As WordPress develops, upgrades may bring about changes that necessitate the update of plugin and theme authors' creations for compatibility. When utilizing an outdated version of WordPress, errors, broken functionality, or even website crashes may occur due to compatibility problems with plugins and themes. This may have an adverse effect on user experience, negatively affect website performance, and make it more difficult to fix compatibility issues.

- Lack of New Features and Improvements: WordPress updates frequently include new features, enhancements, and optimizations that improve your website's usability, functionality, and performance. If you don't update, you may have less customization options, content management options, and user engagement tools available to you. If you aren't using the most recent WordPress capabilities, your website may suffer in comparison to rivals who do.
- Limited Resources and Support: The WordPress community, which consists of users, developers, and designers, actively promotes the platform by offering materials, guidance, and support. However, the most recent iterations of WordPress are the ones that receive the most community support. Your ability to access current support, documentation, tutorials, and troubleshooting tools may be hampered if you're using an outdated version. This may make it more difficult to fix problems, put new features into place, or keep up with industry best practices.

Steps to Reproduce

Normally, you would need to perform the following procedures in order to replicate an outdated version of WordPress:

- Installation: Rather than starting with the most recent version of WordPress, install an earlier version first. Previous versions of WordPress can be found on the official WordPress website or via reliable third parties.
- Decide on the Version: Choose the version of WordPress that you want to use from the list. Find the version's release number or date if you want to copy it.
- Get the WordPress package here: Find the installation package for the WordPress version you want to use and download it. To avoid downloading any corrupted or altered files, be sure you are doing it from a reliable source.
- Create a conducive environment: The installation of WordPress by setting up the environment. This normally entails installing PHP on your own machine or a hosting environment, together with a web server (such as Apache or Nginx), a database server (such as MySQL or MariaDB), and other software.
- Database Creation: To create a new database for your WordPress installation, go here. Usually, you may do this using the command line or the database management tool that your hosting provider offers.

- Extract and Upload Files: Downloaded WordPress packages can be extracted, then the files are uploaded to a web server or hosting environment. To move the files to the right location, you can use an FTP client or file manager that your hosting provider offers.
- Configuration: Input the URL of the location where you uploaded the files to access the WordPress installation through a web browser. To set up the database connection, enter site details, and create an administrative account, adhere to the on-screen instructions.
- Complete Installation: Keep through with the installation procedure until you have a WordPress website that is operational and using the older version you choose.

Proposed mitigation

The following steps are advised in order to reduce the hazards brought on by an outdated WordPress version:

- Updates on a regular basis: Keep WordPress installation current by swiftly implementing new updates and security patches. This guarantees that the most recent security upgrades are in place as well as the patching of identified vulnerabilities.
- Update installed plugins and themes frequently to make sure they are compatible with the newest release of WordPress. Security flaws can also be caused by exploiting vulnerabilities in plugins or themes.
- Monitoring Vulnerabilities: Keep up to date on any new security flaws impacting WordPress and any related plugins and themes. Keep an eye on security warnings and sign up for update notifications to stay on top of new dangers.
- Discard Unused Plugins and Themes: Discard any plugins or themes that are no longer being used by your WordPress installation. Inactive plugins and themes that still have security flaws could be dangerous.
- Strong Passwords and User Access Control: Ensure that all user accounts have strong passwords, and only allow people you can trust with administrator privileges. Apply the principle of least privilege, giving users only the access levels required for their particular responsibilities.
- Plugins for security: Take into account using trustworthy security plugins created especially for WordPress. These plugins can add further levels of security by firewalling, screening for malware, and preventing brute-force attacks.

External Reference

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2022-3590 Detail

Description

WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 5.9 MEDIUM Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2022-3590
NVD Published Date:
12/14/2022
NVD Last Modified:
12/20/2022
Source:
WPScan

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/	Exploit, Third Party Advisory
https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	NIST, WPScan
CWE-918	Server-Side Request Forgery (SSRF)	WPScan

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2023-22622 Detail

Description

WordPress through 6.1.1 depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes "the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner," but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.3 MEDIUM **Vector:** CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-22622
NVD Published Date:
01/04/2023
NVD Last Modified:
02/02/2023
Source:
MITRE

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hypertink	Resource
https://developer.wordpress.org/plugins/cron/	Product Vendor Advisory
https://github.com/WordPress/WordPress/blob/dca7b5204b5fea54e6d1774689777b359a9222ab/wp-cron.php#L5-L8	Third Party Advisory
https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3ae30	Mitigation Third Party Advisory
https://patchstack.com/articles/solving-unpredictable-wp-cron-problems-addressing-cve-2023-22622/	Third Party Advisory
https://wordpress.org/about/security/	Vendor Advisory
https://wordpress.org/support/article/how-to-install-wordpress/	Vendor Advisory
https://www.tenable.com/plugins/was/113449	Third Party Advisory