

Sri Lanka Institute of Information Technology



IT21299902 (ZAKY M.S.M.A)

Bug bounty Report 08.

Domain: merck.com

Web security – IE2062

**B.Sc. (Hons) in Information Technology Specialization in
cyber security.**

Declaration:


- I hereby certify that no part of this assignment has been copied from any other work or any other source. No part of this assignment has been written/produced for me by another person.
- I hold a copy of this assignment that I can produce if the original is lost or damaged.

1. Using components with known vulnerabilities.

- **Outdated version of WordPress (Possible SSRF attack).**

I have identified many vulnerabilities in under domain www.merck.com/. I figured out it has vulnerabilities that listed by OWSAP Top 10. And the overall website risk level is **high**. I used net sparker to identify vulnerabilities in the following domain. And used some of the previously mentioned tools in section. I identified the following OWSAP Top vulnerabilities in following domain.

I hope this message finds you well. I am writing to report a vulnerability I discovered under the domain of <https://www.merck.com/wp-includes/images/arrow-pointer-blue.png> during my participation in the bug bounty program. Please find below the details of the vulnerability for your review and further action.

	Out-of-date Version (WordPress)	GET	https://www.merck.com/wp-includes/images/arrow-pointer-blue.png	HIGH
---	---	-----	---	------

Vulnerability title: outdated version of WordPress (SSRF possible)

Severity: **high**

Affected versions: 6.0.3 to 6.1.1

OWASP classification 2013: A9

CVSS 3.0 score: 6.2

CVSS 3.1 score: 6.2

CVSS string: -

Effectuated components: Word press core.

Database.

Server environment.

Date of Discovery: 2023/05/10

Date of Report: 2023/05/12

2. Vulnerability Description.

I identified that your web application is using an outdated WordPress version. If you keep using this version if an attacker figured out that you are using older version, they will find out the vulnerabilities that version may fall under.

Identified Versions

- 6.0.3, 6.0.2

Latest Version

- 6.0.3 (in this branch)

Vulnerability Database

- Result is based on 05/03/2023 20:30:00 vulnerability database content.

3. Impact assessment.

I have identified the vulnerability that falls under OWSAP top 10 list as Using components with known vulnerabilities. I found it under domain of <https://www.merck.com/>.

Since this is an older version of the software series there are some records that mentioned vulnerabilities in the following version vulnerabilities. Says that this version is vulnerable to **TOCTOU** and **uncontrolled resource consumption** Found this vulnerability under the domain of <https://www.merck.com/wp-includes/images/arrow-pointer-blue.png> version 6.0.3 to 6.1.1 are vulnerable to this attack type.

1. WordPress versions that are out of date are more likely to include security flaws. Attackers may use these flaws to modify data, execute arbitrary commands, introduce malicious code, or obtain unauthorized access. The longer a version is out-of-date, the more likely it is that automated scripts and attackers searching for known vulnerabilities will target it.

🚩 WordPress Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability

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.

Affected Versions

6.0.3 to 6.1.1

🚩 WordPress Uncontrolled Resource Consumption Vulnerability

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.

Affected Versions

6.0.3 to 6.1.1

2. You cannot access the most recent security fixes and upgrades if your WordPress installation is out of date. These upgrades fix known security flaws and aid in shielding your website from prospective attackers. You expose your website to known security dangers by not updating your WordPress version.

3. It's possible that performance optimizations added to current WordPress versions are absent in older versions. It's possible that outdated versions lack performance advancements like caching techniques, database improvements, or code optimizations. As a result, the functionality of your website can be compromised, which might result in slower page loads, a worse user experience, and even lower search engine results.
4. Official support for obsolete WordPress versions gradually decreases over time. This implies that it can be difficult to get support from the WordPress community or developers if you run into any problems or need help. If you continue using an outdated version, you can lose access to vital support tools.

Because of this vulnerability marked as **High** It's a must to address it with a good solution.

4. Steps to Reproduce.

1. Choose the precise WordPress version web application uses and Keep track of the precise version that is vulnerable to uncontrolled resource use.
2. On your website, produce a heavy load or carry out actions that use plenty of resources. This can be done in several ways, including:
 - using tools for load testing, such as Apache JMeter, Siege, or Locust, to simulate a high volume of concurrent user requests. running resource-intensive plugins or themes, or creating posts, uploading files, and performing several simultaneous tasks.
 - sending several queries to vulnerable endpoints or features in a targeted manner.
3. While simulating a heavy load, keep an eye on how your testing environment is using its resources. Monitor database connections and queries, as well as the server's CPU, memory, and disk consumption.
4. Look for evidence that the system resources are not being correctly managed or controlled, such as performance degradation, sluggish response times, server crashes, excessive memory utilization, or other signals.
5. To find any resource-related issues, such as memory leaks, database connection restrictions, or ineffective resource utilization, analyze server logs, performance metrics, and error reports.

5. Proof of existence of the vulnerability.

Identified Versions

- 6.0.3, 6.0.2

Latest Version

- 6.0.3 (in this branch)

Vulnerability Database

- Result is based on 05/03/2023 20:30:00 vulnerability database content.

Request

```
GET /wp-includes/images/arrow-pointer-blue.png HTTP/1.1
Host: www.merck.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 286.9638 Total Bytes Received : 1917 Body Length : 1569 Is Compressed : No

Binary response detected, response has not saved.

6. Proposed mitigation/fix.

1. Updating your WordPress installation to the most recent stable version is the best solution. Security patches, bug fixes, and performance enhancements are frequently included in updates.
2. Check the code of your WordPress theme and plugins for any possible security flaws. usage secure coding techniques to reduce the risk of common vulnerabilities like XSS (Cross-Site Scripting) and SQL injection. These techniques include input validation, output sanitization, and effective usage of WordPress APIs.
3. To add an extra layer of security to your WordPress website, install and set up reliable security plugins. Strong password requirements, the implementation of firewall rules, the detection and mitigation of common vulnerabilities, and routine security scans can all be assisted by these plugins.
4. To find any potential vulnerabilities in your WordPress installation, themes, or plugins, do vulnerability checks periodically using specialist tools like WPScan or security plugins. As soon as vulnerabilities are found, update or replace the impacted components.