Hive Pro

# THREAT ADVISORY

## WordPress fixes multiple security vulnerabilities

**TA2022005**

**Threat Level** AMBER

**Publish Date –** Jan 10, 2022

WordPress development team has released the security update to patch the following four vulnerabilities out of which three of them have high severity.

1. CVE-2022-21661: A vulnerability exists in WP_Query class which is caused due to improper validation of a user-supplied string that is used to construct SQL queries.
2. CVE-2022-21662: A stored cross-site scripting vulnerability that allows an attacker with low privileges (such as authors) to execute JavaScript which might end up affecting users with high privileges.
3. CVE-2022-21663: A security vulnerability allows an attacker with Super Admin role to bypass explicit/additional hardening under certain conditions through object injection.
4. CVE-2022-21664: An SQL injection vulnerability caused due to lack of proper sanitization in one of the classes.

All these vulnerabilities have been fixed in version 5.8.3. Organizations can refer the patch links below to patch these vulnerabilities.

### Vulnerability Details

| CVE ID | Affected Products | Affected CPE | Vulnerability Name | CWE ID |
|---|---|---|---|---|
| CVE-2022-21661 | WordPress Core versions 3.7 to 5.8.0 | cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:* | WordPress WP_Query SQL injection vulnerability | CWE-89 |
| CVE-2022-21662 | WordPress Core versions 3.7 to 5.8.0 | cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:* | WordPress cross-site scripting vulnerability | CWE-79 |
| CVE-2022-21663 | WordPress Core versions 3.7 to 5.8.0 | cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:* | WordPress security bypass vulnerability | CWE-74 |
| CVE-2022-21664 | WordPress Core versions 4.1.34 to 5.8.0 | cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:* | WordPress WP_Meta_Query SQL injection vulnerability | CWE-89 |

### Patch Links

https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/
https://github.com/WordPress/wordpress-develop/commit/c09ccfbc547d75b392dbccc1ef0b4442ccd3c957
https://github.com/WordPress/wordpress-develop/commit/17efac8c8ec64555eff5cf51a3eff81e06317214

### References

https://www.bleepingcomputer.com/news/security/wordpress-583-security-update-fixes-sql-injection-xss-flaws/
https://nvd.nist.gov/vuln/detail/CVE-2022-21661
https://nvd.nist.gov/vuln/detail/CVE-2022-21662
https://nvd.nist.gov/vuln/detail/CVE-2022-21663
https://nvd.nist.gov/vuln/detail/CVE-2022-21664