Severity

Medium

Analysis Summary

CVE-2022-27629 CVSS:4.3

MicroPayments – Paid Author Subscriptions, Content, Downloads, Membership plugin for WordPress is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading an authenticated user to visit a malicious Web site, a remote attacker could send a malformed HTTP request to carry out unintended actions. An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

CVE-2022-27848 CVSS:4.1

Modern Events Calendar Lite plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote authenticated attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

Impact

- Gain Access
- Cross-Site Scripting

Indicator Of Compromise

CVE

- CVE-2022-27629
- CVE-2022-27848

Affected Vendors

WordPress

Affected Products

- WordPress MicroPayments – Paid Author Subscriptions Content Downloads Membership plugin for WordPress 1.9.5
- WordPress MicroPayments – Paid Author Subscriptions Content Downloads Membership plugin for WordPress 1.9.4
- Webnus Modern Events Calendar Lite plugin for WordPress 5.1.6
- Webnus Modern Events Calendar Lite plugin for WordPress 5.1.5
- Webnus Modern Events Calendar Lite plugin for WordPress 6.1.4

Remediation

Upgrade to the latest version of WordPress Plugin, available from the WordPress Plugin Directory.

CVE-2022-27629

CVE-2022-27848