Severity

Medium

Analysis Summary

CVE-2022-29419, CVSS 6

3xSocializer plugin for WordPress is vulnerable to SQL injection. A remote authenticated attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.

CVE-2022-29418, CVSS 5.5

Night Mode plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using the &ntmode_page_setting[enable-me], &ntmode_page_setting[bg-color], &ntmode_page_setting[txt-color], and &ntmode_page_setting[anc_color] parameters 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.

CVE-2022-29417, CVSS 4.3

ShortPixel Adaptive Images plugin for WordPress could allow a remote authenticated attacker to bypass security restrictions, caused by broken access control. An attacker could exploit this vulnerability to change the plugin's settings.

Impact

- Data Manipulation
- Cross-Site Scripting
- Bypass Security

Indicators Of Compromise

CVE

- CVE-2022-29419
- CVE-2022-29418
- CVE-2022-29417

Affected Vendors

WordPress

Affected Products

- WordPress 3xSocializer plugin for WordPress 0.98.22
- WordPress 3xSocializer plugin for WordPress 0.98.21
- WordPress Night Mode plugin for WordPress 1.0.0
- WordPress Night Mode plugin for WordPress 0.9.9
- WordPress Night Mode plugin for WordPress 0.9.8
- WordPress Night Mode plugin for WordPress 0.9.7
- WordPress ShortPixel Adaptive Images plugin for WordPress 3.3.1
- WordPress ShortPixel Adaptive Images plugin for WordPress 3.3.0

Remediation

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

CVE-2022-29419

CVE-2022-29418

CVE-2022-29417