Severity

Medium

Analysis Summary

CVE-2022-0953 CVSS:6.1

Anti-Malware Security and Brute-Force Firewall plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the admin page. A remote attacker could exploit this vulnerability using the QUERY_STRING in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-1153 CVSS:5.5

LayerSlider plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the template slug of any slider. 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

- Cross-Site Scripting

Indicator Of Compromise

CVE

- CVE-2022-0953
- CVE-2022-1153

Affected Vendors

Cross-Site Scripting

Affected Products

WordPress Anti-Malware Security and Bruteforce Firewall plugin for WordPress 4.18.63 WordPress Anti-Malware Security and Brute-Force Firewall plugin for WordPress 4.20.59 WordPress Anti-Malware Security and Brute-Force Firewall plugin for WordPress 4.20.59 KREATURA MEDIA LayerSlider plugin for WordPress 7.1.1

Remediation

Upgrade to the latest version of Anti-Malware Security and Brute-Force Firewall plugin for WordPress and LayerSlider plugin for WordPress, available from the WordPress Web site.

CVE-2022-0953

CVE-2022-1153