Security Advisory 2020-011

Multiple XSS Vulnerabilities in Wordpress Plugins

March 03, 2020 — v1.0

TLP:WHITE

History:

- *03/03/2020 — v1.0 – Initial publication*

Summary

Several cross-site scripting (XSS) vulnerabilities were fond in popular WordPress plugins. Some of them could give attackers complete control of sites [1]. It is to be mentioned that this year we have already observed other vulnerabilities in WordPress plugins [2, 3, 4, 5].

Technical Details

Here is the list of affected plugins and potential impact:

- **Flexible Checkout Fields for WooCommerce** - unauthenticated stored XSS [6]. Unauthenticated attackers are capable of modifying the plugin's options, which can be leveraged to inject XSS payloads that can be triggered in the dashboard of a logged-in administrator.
- **Async JavaScript** - subscriber+ stored XSS [7]. Low-privilege users including *subscribers* can modify the plugin's settings. Certain setting values can be injected with a crafted payload to execute malicious JavaScript when a WordPress administrator views certain areas of their dashboard.
- **10Web Map Builder for Google Maps** - unauthenticated stored XSS [8]. An attacker can inject malicious JavaScript into certain settings values, that code will execute for administrators in their dashboard as well as front-of-site visitors in some circumstances.
- **Modern Events Calendar Lite** - multiple subscriber+ stored XSS Vulnerabilities [9]. Low-privileged users like *subscribers* could manipulate settings and other stored data. When exploited in this way, the affected data can be injected with various XSS payloads. It may allow creation of rogue accounts for the attackers.

Recommendations

It is highly recommended to update the plugins to the latest version as soon as possible as there were reported hacked sites [10].

- Unauthenticated Stored XSS in Flexible Checkout Fields For WooCommerce. Patched Version: 2.3.2
- Subscriber+ Stored XSS in Async JavaScript. Patched Version: 2.20.02.27
- Unauthenticated Stored XSS in 10Web Map Builder for Google Maps. Patched Version: 1.0.64
- Multiple Subscriber+ Stored XSS Vulnerabilities In Modern Events Calendar Lite. Patched Version: 5.1.7

References

[1] https://www.wordfence.com/blog/2020/02/site-takeover-campaign-exploits-multiple-zero-day-vulnerabilities/

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-005.pdf

[3] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-007.pdf

[4] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-008.pdf

[5] https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-009.pdf

[6] https://www.wpdesk.net/blog/flexible-checkout-fields-vulnerability/

[7] https://wpvulndb.com/vulnerabilities/10098

[8] https://wpvulndb.com/vulnerabilities/10099

[9] https://wpvulndb.com/vulnerabilities/10100

[10] https://nakedsecurity.sophos.com/2020/03/03/xss-plugin-vulnerabilities-plague-wordpress-users/