Ram Gall

April 7, 2020

Critical Vulnerabilities in the WP Lead Plus X WordPress Plugin

On March 3, 2020, our Threat intelligence team discovered a number of vulnerabilities in WP Lead Plus X, a WordPress plugin with over 70,000 installations designed to allow site owners to create landing and squeeze pages on their sites. These vulnerabilities allowed an authenticated attacker with minimal permissions, such as a subscriber, to create or completely replace any page on a site with their own page containing malicious JavaScript, defacement, or a redirect. Additionally, an unauthenticated attacker could also upload a malicious page template which, if used by an administrator running the premium version of the plugin, would execute malicious JavaScript in that administrator's browser, potentially leading to site takeover.

We attempted to contact the plugin's author the next day, on March 4, 2020, followed up on March 12, 2020, and privately sent the full vulnerability disclosure. The plugin's author released a preliminary patch containing capability checks on March 15th. We followed up with them the next day as the patched version was still vulnerable to Cross-Site Request Forgery (CSRF), and were informed that a more complete patch would be forthcoming. More than 2 weeks later, and more than a month after our initial contact attempt, the complete patch is not yet available.

If this plugin is critical to your site's functionality, we highly recommend updating to at least version 0.99 immediately as at least some of these security issues are patched in that version. Ideally, we recommend disabling and deleting this plugin until a more complete patch becomes available.

Wordfence Premium users received a new firewall rule on March 4, 2020 to protect against exploits targeting these vulnerabilities. Users still using the free version of Wordfence will receive this rule on April 3, 2020.

Description: Authenticated Stored Cross-Site Scripting(XSS)
Affected Plugin: Landing Page – Squeeze Page – Responsive Landing Page Builder Free – WP Lead Plus X
Plugin Slug: free-sales-funnel-squeeze-pages-landing-page-builder-templates-make
Affected Versions: <= 0.98
CVE ID: CVE-2020-11508
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L
CVSS Score: 9.1(Critical)
Patched Version: 0.99

WP Lead Plus X is a WordPress plugin that allows site owners to create custom landing and "squeeze" pages, complete with its own page builder interface capable of inserting custom JavaScript. Unfortunately, this page builder interface also relied on an unprotected AJAX function which lacked a capability check and a nonce check in order to save and update pages:

```
add_action('wp_ajax_core37_lp_save_page', 'core37_lp_save_page');

function core37_lp_save_page()
{
    $content = array();
    parse_str(file_get_contents("php://input"), $content);

    //pass the form ID to the editor
    echo Page_Manager::save_page($content);
    die();
}
```

As such, it was possible for a logged-in attacker with minimal permissions (such as a subscriber) to send a `$_POST` request to `wp-admin/admin-ajax.php` with the `action` parameter set to `core37_lp_save_page` along with the `pageContent`, `pageSlug`, `pageTitle`, and `pageSettings` parameters describing the page to be created. This included the page title, page slug, page content, and any JavaScript the attacker wanted to execute when the page loaded.

Worse yet, if a `pageID` parameter was sent with the ID of an existing page or post, that page or post would be completely replaced by the malicious page. This made it possible for an attacker to completely replace every single post or page on a site, including revision backups, with their own malicious content, with no way to revert other than restoring content from a database backup.

In addition to inserting malicious JavaScript, which on its own could be used to redirect visitors to malvertising sites or steal sensitive information, this vulnerability could be used to effectively turn any site running the plugin into a spam site.

Description: Unauthenticated Stored Cross-Site Scripting (XSS)
Affected Plugin: Landing Page – Squeeze Page – Responsive Landing Page Builder Free – WP Lead Plus X
Plugin Slug: free-sales-funnel-squeeze-pages-landing-page-builder-templates-make
Affected Versions: <= 0.98
CVE ID: CVE-2020-11509
CVSS Vector:CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
CVSS Score: 7.1(High)
Patched Version: 0.99

One of the features available to users who have paid for a license key for WP Lead Plus X is the ability to create and use "template" pages, which can be imported as a starting point when creating new pages. Although this feature is not visible if the plugin does not have a license key, it was still possible for an unauthenticated user to import a template containing malicious JavaScript. This was due to an `admin_post` action available to unprivileged visitors:

```
add_action('admin_post_nopriv_c37_wpl_import_template', array($this, 'c37_wpl_import_template'));
```

Additionally, the function called by this action lacked nonce or capability checks:

```
public function c37_wpl_import_template()
{
```

```
                Template_Manager::importTemplateFromString(file_get_contents($tmpFile));
            }
        }

        wp_redirect($_POST['request_url'] . '&import=success');
}
```

As such, it was possible for an unauthenticated attacker to upload a template by sending a `$_POST` request to `wp-admin/admin-post.php`, with the `action` parameter set to `c37_wpl_import_template` and a `files_name[]` parameter containing a maliciously crafted template file. If a site owner with a licensed copy of the plugin used this imported template to create a page, the malicious JavaScript would execute in their browser, potentially leading to site takeover.

Description: Cross-Site Request Forgery(CSRF)
Affected Plugin: Landing Page – Squeeze Page – Responsive Landing Page Builder Free – WP Lead Plus X
Plugin Slug: free-sales-funnel-squeeze-pages-landing-page-builder-templates-make
Affected Versions: <= 0.99
CVE ID: Pending
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H
CVSS Score: 8.3(High)
Patched Version: N/A

As mentioned previously, none of the functions in this plugin use nonce checks, so it is possible for an attacker to perform any action that the plugin is capable of by tricking an administrator into clicking a specially crafted link designed to perform that action. This includes all the capabilities described above, including adding pages to the site, replacing site content with malicious JavaScript, and more.

What should I do?

This is an unusual situation in that the plugin has not yet been fully patched. It is still vulnerable to a CSRF attack. Additionally, firewalls (including the Wordfence Web Application Firewall) cannot protect a site against a CSRF attack as these attacks look like valid requests to your site. If you manage a site with this plugin installed, this means that the security of your site is precariously in your hands, and the hands of anyone with administrator rights to your site. CSRF attacks require the victim's participation, usually by clicking a crafted link in an email. If this plugin is absolutely critical to your site's functionality, we urge you to upgrade to the latest available version and exercise extreme caution when visiting any links, especially those sent to you in email messages. If you're not actively using this plugin, we recommend disabling it and removing it until a more complete patch is available.

Disclosure Timeline

March 3, 2020 – Wordfence Threat Intelligence discovers and analyzes vulnerabilities in the WP Lead Plus X plugin.
March 4, 2020 – Firewall rule released for Wordfence Premium users. Initial outreach to plugin developer.
March 12, 2020 – Followup with developer as no response was received. Developer confirms appropriate inbox for handling discussion. Full disclosure of vulnerabilities is sent.
March 15, 2020 – Plugin developer releases initial patch including capability checks.
March 16, 2020 – Followup with developer as patched version is still vulnerable to CSRF. Developer replies that a fix for CSRF issues is forthcoming.
April 3, 2020 – Firewall rule becomes available to Wordfence free users.

Conclusion

In today's post, we detailed two stored XSS vulnerabilities in the WP Lead Plus X plugin, as well as a CSRF vulnerability. The XSS flaws have been patched in version 0.99 and we recommend that users that rely on this plugin update to the latest version available immediately. The CSRF vulnerability has not yet been patched, and we recommend that users that can do so deactivate and delete this plugin until a more complete patch is available.

Sites running Wordfence Premium have been protected from attacks against the XSS vulnerabilities since March 4, 2020. Sites running the free version of Wordfence received the same firewall rule update on April 3, 2020.
Did you enjoy this post? Share it!

Comments

No Comments

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service Privacy Policy

CCPA Privacy Notice

Products

Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence Central

Support

Documentation
Learning Center
Free Support
Premium Support

News

Blog
In The News
Vulnerability Advisories

About

About Wordfence
Careers
Contact
Security
CVE Request Form