NinTechNet

The Ninja Technologies Network

MENU

Zero-day vulnerability exploited in WordPress Lara Google Analytics plugin.

BY JEROME BRUANDET OCTOBER 14, 2019 - 4:47PM [+0700]

The WordPress Lara Google Analytics plugin, which has 20,000+ active installations, was prone to an authenticated stored XSS vulnerability in version 2.0.4 and below.

> This vulnerability is currently being exploited, make sure to follow the recommendations below.

Reference

A CVE ID has been requested and we'll update this post when it is assigned.

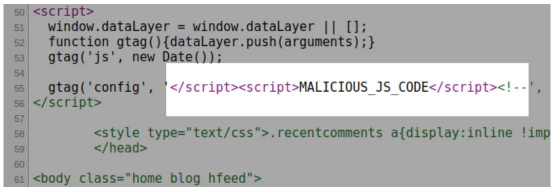
Authenticated Stored XSS

In the main "lara-google-analytics.php" script, the `lrgawidget_setProfileID` action is used to call the `lrgawidget_callback` function via the WordPress AJAX API.

```
add_action( 'wp_ajax_lrgawidget_setProfileID', 'lrgawidget_callback
...
...
function lrgawidget_callback() {
   global $wpdb;
   $user_id = get_current_user_id();
   $lrperm = lrgawidget_internal_permissions();
   $lrdata = $_POST;
   $modifiedAction = explode("_", $lrdata['action']);
   $lrdata['action'] = $modifiedAction[1];

   if ($lrdata['action'] == "setProfileID"){
      if ( (isset($lrdata['enable_universal_tracking'])) && !empty(
         update_option('lrgawidget_property_id', $lrdata['property_
      }else{
         delete_option('lrgawidget_property_id');
      }
   }
```

Attackers are using it to inject JS code in the `property_id` field. It is injected into all pages and posts of the CMS:



```
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', '</script><script>MALICIOUS_JS_CODE</script><!--',
</script>

        <style type="text/css">.recentcomments a{display:inline !imp
        </head>

<body class="home blog hfeed">
```

Note that the attack requires a user account on the blog, such as a subscriber.

Timeline

The vulnerability was reported to the wordpress.org team on October 13, 2019, and a new version 2.0.5 was released the same day.

Recommendations

Update as soon as possible if you have version 2.0.4 or below installed. Note that the new version was released only a few hours after we reported the issue – which is a great thing – and it does block the ongoing attack, however it still lacks capability check and hopefully the author will come up with a better patch in the next few days.

If you are using our web application firewall for WordPress, NinjaFirewall WP Edition (free) and NinjaFirewall WP+ Edition (premium), you are protected against this vulnerability.

Stay informed about the latest vulnerabilities in WordPress plugins and themes: @nintechnet

TAGGED: NINJAFIREWALL, SECURITY, VULNERABILITY, WORDPRESS

PREVIOUS

Stored XSS vulnerability in WordPress Download Plugins and Themes from Dashboard plugin.

NEXT

Multiple vulnerabilities in Sliced Invoices plugin.

OUR PRODUCTS

NinjaFirewall WP+

Web Application Firewall for WordPress. It will give your blog the highest level of protection it deserves.

FREE DOWNLOAD

NinjaFirewall Pro+

Web Application Firewall for PHP applications. It will protect your PHP site, from custom scripts to popular shopping cart and CMS applications.

FREE DOWNLOAD

NinjaScanner

A lightweight, fast and powerful Antimalware scanner for WordPress which includes many features to help you scan your blog for malware and virus.

FREE DOWNLOAD

Code Profiler

Speed up your WordPress website by locating bottlenecks and performance issues in your plugins and themes.

FREE DOWNLOAD

CATEGORIES

Select Category

SEARCH

Search …

RECENT POSTS

1. WordPress FlyingPress plugin fixed broken access control vulnerability.
   November 28, 2022 - 12:13pm [+0700]
2. 8 WordPress plugins fixed high severity vulnerability.
   April 12, 2022 - 11:48am [+0700]
3. Unauthenticated function injection vulnerability in WordPress Sparkling theme.
   February 10, 2022 - 5:41pm [+0700]
4. Critical vulnerability in WordPress AdSanity plugin.
   January 25, 2022 - 12:17pm [+0700]
5. Code Profiler: WordPress Website Performance Profiling Made Easy.
   December 19, 2021 - 1:48am [+0700]