DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress WebDorado Gallery Plugin
SQL Injection Vulnerability

WordPress WebDorado Gallery Plugin – SQL Injection Vulnerability	
Advisory ID:	**DC-2017-02-011**
Software:	**WordPress WebDorado Gallery Plugin**
Software Language:	**PHP**
Version:	**1.3.29 and below**
Vendor Status:	**Vendor contacted, vulnerability confirmed**
Release Date:	**20170502**
Risk:	**Medium**

1. General Overview

During the security audit, multiple security vulnerabilities were discovered in WordPress WebDorado Gallery Plugin using DefenseCode ThunderScan application source code security analysis platform.

More information about ThunderScan is available at URL:
http://www.defensecode.com

2. Software Overview

According to the plugin developers, WebDorado, Gallery plugin is a fully responsive WordPress gallery plugin with advanced functionality that is easy to customize and has various views. It has more than 300,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/photo-gallery/
https://web-dorado.com/products/wordpress-photo-gallery-plugin.html

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in WebDorado Gallery WordPress plugin. The easiest way to reproduce the vulnerability is to visit the provided URL while being logged in as administrator or another user that is authorized to access the plugin settings page. Any user with such privileges can obtain the valid bwg_nonce value by previously visiting the settings page. Users that to do not have full administrative privileges could abuse the database access the vulnerability provides to either escalate their privileges or obtain and modify database contents they were not supposed to be able to.

3.1 SQL injection	
Function:	**$wpdb->get_col($query)**
Variable:	**$_GET['album_id']**

Sample URL:

```
http://www.vulnerablesite.com/wp-admin/admin-ajax.php?action=addAlbumsGalleries&album_id=0%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(5)))VvZV)&width=700&height=550&bwg_items_per_page=20&bwg_nonce=b939983df9&TB_iframe=1
```

File: photo-gallery\admin\models\BWGModelAddAlbumsGalleries.php

```
$album_id = ((isset($_GET['album_id'])) ? esc_html(stripslashes($_GET['album_id'])) : ((isset($_POST['album_id'])) ? esc_html(stripslashes($_POST['album_id'])) : ''));
...
$page_nav = $this->model->page_nav($album_id);
```

File: photo-gallery\admin\views\BWGViewAddAlbumsGalleries.php

```
public function page_nav($album_id) {
...
$query = "SELECT id FROM " . $wpdb->prefix . "bwg_album WHERE published=1 AND id<>" . $album_id . " " . $where . " UNION ALL SELECT id FROM " . $wpdb->prefix . "bwg_gallery WHERE published=1 " . $where;
$total = count($wpdb->get_col($query));
```

4. Solution

Vendor resolved the security issues in one of the subsequent releases. All users are strongly advised to update WordPress WebDorado Gallery plugin to the latest available version. Version 1.3.38 no longer seems to be vulnerable.

5. Credits

Discovered by Neven Biruski with DefenseCode ThunderScan source code security analyzer.

6. Disclosure Timeline

20170404	**Vendor contacted**
20170405	**Vendor responded: *"Thanks for noticing and told us about this, we will take into account and will fix the issues with upcoming update."***
?	**Update released**
20170502	**Latest plugin version tested. Vulnerability seems fixed. Advisory released to the public.**

7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/