

# DefenseCode



## DefenseCode ThunderScan SAST Advisory

### WordPress Huge-IT Video Gallery Plugin Security Vulnerability

Huge-IT Video Gallery – SQL injection Security Vulnerability	
Advisory ID:	<b>DC-2017-01-009</b>
Software:	<b>Huge-IT Video Gallery</b>
Software Language:	<b>PHP</b>
Version:	<b>2.0.4 and below</b>
Vendor Status:	<b>Vendor contacted, update released</b>
Release Date:	<b>2017/05/24</b>
Risk:	<b>High</b>

#### 1. General Overview

During the security audit of Huge-IT Video Gallery plugin for WordPress CMS, security vulnerability was discovered 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 developers, Gallery Video plugin was created and specifically designed to show video links in unusual splendid gallery types supplemented of many gallery options.

According to wordpress.org, it has more than 40,000 active installs.

Homepage:

<https://wordpress.org/plugins/gallery-video/>

<http://huge-it.com/wordpress-video-gallery/>

### 3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Huge-IT Video 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. Users that 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.

Due to the missing nonce token, the attacker the vulnerable code is also directly exposed to attack vectors such as Cross Site request forgery (CSRF).

#### 3.1 SQL injection

Vulnerable Function: **`$wpdb->get_var( $query );`**  
Vulnerable Variable: **`$_POST['cat_search']`**

Vulnerable URL:

```
http://www.vulnerablesite.com/wp-admin/admin.php?page=video_galleries_huge_it_video_gallery
```

Vulnerable body:

```
cat_search=DefenseCode AND (SELECT * FROM (SELECT(SLEEP(5)))DC)
```

File: gallery-video\includes\admin\class-gallery-video-galleries.php

```
107 $cat_id = sanitize_text_field( $_POST['cat_search'] );  
...  
118 $where .= " AND sl_width=" . $cat_id;  
...  
127 $query = "SELECT COUNT(*) FROM ".$wpdb->prefix."huge_it_videogallery_galleries".$where;  
128 $total = $wpdb->get_var( $query );
```

### 4. Solution

Vendor resolved the security issues. All users are strongly advised to update WordPress Huge-IT Video Gallery plugin to the latest available version.

### 5. Credits

Discovered with DefenseCode ThunderScan Source Code Security Analyzer by Neven Biruski.

### 6. Disclosure Timeline

2017/03/31	<b>Vendor contacted</b>
2017/04/06	<b>Vendor responded</b>
2017/05/24	<b>Advisory released to the public</b>

### 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](mailto:defensecode@defensecode.com)

Website: <http://www.defensecode.com>

Twitter: <https://twitter.com/DefenseCode/>