DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Top-10 Plugin
SQL Injection Security Vulnerability

WordPress Top-10 Plugin – SQL injection Security Vulnerability	
Advisory ID:	**DC-2017-12-003**
Software:	**WordPress Top-10 plugin**
Software Language:	**PHP**
Version:	**2.4.2 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/12/13**
Risk:	**High**

1. General Overview

During the security audit of Top-10 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 plugin developers, Top-10 WordPress plugin can count daily and total visits per post and display the most popular posts based on the number of views.

According to wordpress.org, it has more than 30,000 active installs.

Homepage:
https://wordpress.org/plugins/Top-10/
https://webberzone.com/plugins/Top-10/

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Top-10 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.

3.1 SQL injection	
Vulnerable Function:	**$wpdb->get_results($sql, 'ARRAY_A')**
Vulnerable Variable:	**$_REQUEST['orderby']**

File: Top-10\admin\class-stats.php

```
111     $orderby = sanitize_text_field( wp_unslash( $_REQUEST['orderby'] ) );
...
134     $sql = "SELECT $fields FROM {$table_name} $join WHERE 1=1 $where $groupby $orderby
$limits";
…
136   $result = $wpdb->get_results( $sql, 'ARRAY_A' );
```

4. Solution

After the vulnerability was reported the vendor resolved the security issues. All users are strongly advised to update WordPress Top-10 plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2017/04/04	**Vendor contacted**
2017/04/05	**Vendor responded**
2017/04/07	**Update released**
2017/12/13	**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/