DefenseCode ThunderScan SAST Advisory

53+ WordPress plugins by BestWebSoft Multiple Cross-Site Scripting (XSS) Vulnerabilities

<table>
<tr><th colspan="2">53+ WordPress plugins by BestWebSoft - Multiple Cross-Site Scripting (XSS) Vulnerabilities</th></tr>
<tr><td>Advisory ID:</td><td><b>DC-2017-02-014</b></td></tr>
<tr><td>Software:</td><td><b>53+ WordPress plugins by BestWebSoft</b></td></tr>
<tr><td>Software Language:</td><td><b>PHP</b></td></tr>
<tr><td>Version:</td><td><b>Various</b></td></tr>
<tr><td>Vendor Status:</td><td><b>Vendor contacted, vulnerabilities confirmed</b></td></tr>
<tr><td>Release Date:</td><td><b>20170412</b></td></tr>
<tr><td>Risk:</td><td><b>Medium</b></td></tr>
</table>

1. General Overview

During the security audit, multiple security vulnerabilities were discovered in 53+ WordPress plugins by BestWebSoft using DefenseCode ThunderScan application source code security analysis platform.

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

2. Software Overview

BestWebSoft published more than 50 plugins to the wordpress.org site. Almost all plugins contain the Panel - a component designed for overview and management of various BestWebSoft plugins - both the ones that are installed and the ones that are available for download. That's the component that's vulnerable to the Cross-site scripting attacks.

According to wordpress.org, there are more than 850,000 active installs of plugins with the vulnerable Panel component.

Homepage:
https://bestwebsoft.com/products/wordpress/plugins/
https://profiles.wordpress.org/bestwebsoft/#content-plugins

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross Site Scripting vulnerabilities in 53 BestWebSoft plugins that were published on the wordpress.org web site. Vulnerabilities were discovered in the administrative section of the plugins. The Cross-Site Scripting vulnerability can enable the attacker to construct the URL that contains malicious JavaScript code. If the administrator of the site makes a request to such an URL, the attacker's code will be executed, with unrestricted access to the WordPress site in question.

The attacker can entice the administrator to visit the URL in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum, or embedding it as an IMG tag source in another web page administrator will visit, causing the administrator's browser to request the URL automatically (due to missing nonce token the vulnerability is directly exposed to Cross site request forgery, CSRF, attacks).

In any case, after the administrator's browser visits such an URL and automatically executes the attacker's JavaScript code, the attacker should be able to acquire administrator privileges for himself with ease.

As of 20170224, the vulnerable plugins and appropriate versions are as follows:

Plugin name	Version	Active Installs	Plugin Short Name
Google AdSense	v1.43	10000+	(adsense-plugin)
Featured Posts	v1.0.0	400+	(bws-featured-posts)
Google Analytics	v1.7.0	6000+	(bws-google-analytics)
Google Maps	v1.3.5	800+	(bws-google-maps)
Latest Posts	v0.2	200+	(bws-latest-posts)
LinkedIn	v1.0.4	200+	(bws-linkedin)
Pinterest	v1.0.4	600+	(bws-pinterest)
Popular Posts	v1.0.3	900+	(bws-popular-posts)
SMTP	v1.0.9	2000+	(bws-smtp)
Testimonials	v0.1.8	500+	(bws-testimonials)
Captcha	v4.2.8	300000	(captcha)
Car Rental	v1.0.4	200+	(car-rental)
Contact Form Multi	v1.2.0	2000+	(contact-form-multi)
Contact Form	v4.0.4	200000	(contact-form-plugin)
Contact Form to DB	v1.5.6	3000+	(contact-form-to-db)
Custom Admin Page	v0.1.1	200+	(custom-admin-page)
Custom Fields Search	v1.3.1	3000+	(custom-fields-search)
Custom Search	v1.35	2000+	(custom-search-plugin)
Donate	v2.1.0	700+	(donate-button)
Email Queue	v1.1.1	80+	(email-queue)
Error Log Viewer	v1.0.5	500+	(error-log-viewer)
Facebook Button	v2.53	30000+	(facebook-button-plugin)
Gallery Categories	v1.0.7	3000+	(gallery-categories)
Gallery	v4.4.9	70000+	(gallery-plugin)
Google Captcha	v1.27	70000+	(google-captcha)
Google +1	v1.3.3	1000+	(google-one)
Google Shortlink	v1.5.2	600+	(google-shortlink)
Google Sitemap	v3.0.7	90000+	(google-sitemap-plugin)
Htaccess	v1.7.5	800+	(htaccess)

Job Board	v1.1.3	500+	(job-board)
Limit Attempts	v1.1.7	10000+	(limit-attempts)
Multilanguage	v1.2.1	10000+	(multilanguage)
Pagination	v1.0.6	5000+	(pagination)
PDF & Print	v1.9.3	9000+	(pdf-print)
Portfolio	v2.39	6000+	(portfolio)
Post to CSV	v1.3.0	600+	(post-to-csv)
Profile Extra Fields	v1.0.6	500+	(profile-extra-fields)
PromoBar	v1.1.0	200+	(promobar)
Quotes and Tips	v1.31	800+	(quotes-and-tips)
Rating	v0.1	90+	(rating-bws)
Re-attacher	v1.0.8	2000+	(re-attacher)
Reality	v1.0.9	400+	(realty)
Relevant - Related	v1.1.9	1000+	(relevant)
Sender	v1.2.0	700+	(sender)
Social Buttons Pack	v1.1.0	2000+	(social-buttons-pack)
Social Login	v0.1	10+	(social-login-bws)
Subscriber	v1.3.4	6000+	(subscriber)
Timesheet	v0.1.4	90+	(timesheet)
Twitter Button	v2.53	7000+	(twitter-plugin)
Updater	v1.34	9000+	(updater)
User Role	v1.5.5	4000+	(user-role)
Visitors Online	v0.9	2000+	(visitors-online)
Zendesk Help Center	v1.0.4	30+	(zendesk-help-center)

3.1 Cross-Site Scripting

Function:	**Echo**
Variable:	**$_GET['category']**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=bws_panel&category="></script><script>alert(42)</script>
```

File: PLUGIN_DIR/bws_menu/bws_menu.php

```
…
$plugin_category = isset( $_GET['category'] ) ? $_GET['category'] : 'all';
<li><a <?php if ( ! isset( $_GET['sub'] ) ) echo 'class="current" '; ?>href="<?php echo
$current_page; if ( 'all' != $plugin_category ) echo '&amp;category=' . $plugin_category;
?>"><?php _e( 'All', 'bestwebsoft' ); ?></a></li> |
…
```

3.2 Cross-Site Scripting

Function:	**Echo**
Variable:	**$_GET['category']**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=bws_panel&category="></script><script>alert(42)</script>&sub=installed
```

File: PLUGIN_DIR/bws_menu/bws_menu.php

```
…
```

```
$plugin_category = isset( $_GET['category'] ) ? $_GET['category'] : 'all';
<li><a <?php if ( isset( $_GET['sub'] ) && 'installed' == $_GET['sub'] ) echo
'class="current" '; ?>href="<?php echo $current_page; ?>&amp;sub=installed <?php if ( 'all'
!= $plugin_category ) echo '&amp;category=' . $plugin_category; ?>"><?php _e( 'Installed',
'bestwebsoft' ); ?></a></li> |
…
```

3.3 Cross-Site Scripting

Function:	**Echo**
Variable:	**$_GET['category']**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=bws_panel&category="></script><script>alert(42)</script>&sub=not_installed
```

File: PLUGIN_DIR/bws_menu/bws_menu.php

```
…
$plugin_category = isset( $_GET['category'] ) ? $_GET['category'] : 'all';
<li><a <?php if ( isset( $_GET['sub'] ) && 'not_installed' == $_GET['sub'] ) echo
'class="current" '; ?>href="<?php echo $current_page; ?>&amp;sub=not_installed<?php if (
'all' != $plugin_category ) echo '&amp;category=' . $plugin_category; ?>"><?php _e( 'Not
Installed', 'bestwebsoft' ); ?></a></li>
…
```

4. Solution

Vendor responded:

We have already known about this vulnerability and some plugins have already been fixed. We will fix the rest of the plugins in their future updates.

All users are strongly advised to update their WordPress plugins to the latest available version.

5. Credits

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

6. Disclosure Timeline

24/03/2017	**Vendor contacted**
27/03/2017	**Advisory sent to vendor**
28/03/2017	**Vendor responded and confirmed the vulnerability**
12/04/2017	**Advisory released to the public**

7. About DefenseCode ThunderScan

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/