DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Gwolle Guestbook Plugin
XSS Security Vulnerability

WordPress Gwolle Guestbook Plugin – XSS Security Vulnerability	
Advisory ID:	**DC-2018-05-008**
Software:	**WordPress Gwolle Guestbook plugin**
Software Language:	**PHP**
Version:	**2.5.3 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2018/07/24**
Risk:	**Medium**

1. General Overview

During the security audit of Gwolle Guestbook 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, Gwolle Guestbook is is not just another guestbook for WordPress. The goal is to provide an easy and slim way to integrate a guestbook into your WordPress powered site.

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

Homepage:
https://wordpress.org/plugins/gwolle-gb/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting vulnerability in Gwolle Guestbook WordPress plugin.

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.

To confirm the vulnerability make sure dashboard widget is added and that there is at least one unchecked entry in the guestbook. The vulnerability was tested using Apache web server.

3.1 Cross-Site Scripting	
Vulnerable Function:	**echo()**
Vulnerable Variable:	**$_SERVER['PHP_SELF']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/index.php/"></script><script>alert(42)</script>
```

File: gwolle-gb/admin/gb-dashboard-widget.php

```
150 <a href="<?php echo $_SERVER['PHP_SELF']; ?>" class="button"><?php esc_html_e('Refresh',
'gwolle-gb'); ?></a>
```

4. Solution

All users are strongly advised to update WordPress Gwolle Guestbook plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2018/06/01	**Vulnerability discovered**
2018/06/05	**Vendor contacted**
2018/07/24	**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/