DefenseCode

DefenseCode WebScanner DAST Advisory

WordPress User Access Manager Plugin Cross-Site Scripting (XSS) Vulnerability

WordPress User Access Manager Plugin –Cross-Site Scripting (XSS) Vulnerability	
Advisory ID:	**DC-2017-01-021**
Software:	**WordPress User Access Manager plugin**
Software Language:	**PHP**
Version:	**1.2.14 and below**
Vendor Status:	**Vendor contacted, vulnerability fixed**
Release Date:	**20170510**
Risk:	**Medium**

1. General Overview

During the security audit, multiple security vulnerabilities were discovered in WordPress User Access Manager plugin using DefenseCode WebScanner web application security analysis platform.

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

2. Software Overview

According to the developers, User Access Manager plugin can be used to manage the access to your posts, pages, categories and files.

It has more than 40,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/user-access-manager/

3. Vulnerability Description

During the security analysis, WebScanner discovered Cross Site Scripting vulnerability in User Access Manager 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. Due to missing nonce token the vulnerability is also directly exposed to other, indirect attack vectors.

3.1 Cross-Site Scripting	
Function:	**echo()**
Variable:	**$_GET['id']**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=uam_usergroup&action=editGroup&id=%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

File: user-access-manager\tpl\adminGroup.php

```
443   $groupId = $_GET['id'];
444   getPrintEditGroup($groupId);
...
67    function getPrintEditGroup($sGroupId = null)
...
83    <input type="hidden" value="<?php echo $sGroupId; ?>" name="userGroupId" />
```

4. Solution

Vendor resolved security issues in the next release (2.0.0). All users are strongly advised to update WordPress User Access Manager plugin to the latest available version.

5. Credits

Discovered by Neven Biruski with DefenseCode WebScanner web application security analysis platform.

6. Disclosure Timeline

04/04/2017	**Vendor contacted**
12/04/2017	**Vendor responded. Asked us for a bit more time.**
23/04/2017	**Update released**
09/05/2017	**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/