Multiple XSS Vulnerabilities in Prestashop

Title: Multiple XSS Vulnerabilities in Prestashop
Release Date: 2011/11/22
Vulnerable Application: Prestashop (ver. 1.4.4.1)
Type: Cross Site Scripting
Level: High (Low/High/Critical)
CVSS: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Dognædis Ref.: DGS-SEC-6
CVE Ref.: CVE-2011-4544
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): SAlves
Contact: irt@dognaedis.com

Overview:

PrestaShop is an e-commerce solution which is free for the basic kernel and open source. It supports payment gateways such as Google checkout, Paypal or payments pro via APIs.

Scope:

File: /modules/mondialrelay/googlemap.php

Vulnerable Argument(s): $_GET['address'] and $_GET['relativ_base_dir']

Code:

```
line 29: geocoder.geocode( {'address': "<?php echo $_GET['address']; ?>"}, function(results, status)
...
line 39: infowindow.setContent("<?php echo $_GET['address']; ?>");
...
line 52: var image = new google.maps.MarkerImage('<?php echo $_GET['relativ_base_dir'];
?>modules/mondialrelay/kit_mondialrelay/marker.gif');
...
line 59: infowindow.setContent('<img src="<?php echo $_GET['relativ_base_dir'];
?>modules/mondialrelay/kit_mondialrelay/MR_small.gif" />' + ' ' + address);
```

Proof(s) of Concept:

```
GET: http://<app_base>/modules/mondialrelay/googlemap.php?relativ_base_dir=>');alert('XSS');//
GET: http://<app_base>/modules/mondialrelay/googlemap.php?relativ_base_dir=">');alert('XSS');//
Note: To trigger the vulnerability on the lines 39 and 59, the user has to click on the googlemaps
marker.
```

File: /prestashop/modules/mondialrelay/googlemap.php

Vulnerable Argument(s): $_GET['relativ_base_dir'], $_GET['Pays'], $_GET['Ville'], $_GET['CP'], $_GET['Poids'], $_GET['Action'] and $_GET['num']

Code:

```
line 100:
recherche_MR(\'relativ_base_dir='.$_GET['relativ_base_dir'].'&Pays='.$_GET['Pays'].'&Ville='.$_GET['Ville
'].'&CP='.$_GET['CP'].'&Taille=&Poids='.$_GET['Poids'].'&Action='.$_GET['Action'].'&num='.$_GET['num'].'\
');
```

Proof(s) of Concept:

```
GET: http://<app_base>/modules/mondialrelay/googlemap.php?Pays=');alert('XSS');//
```

Description:

The referred vulnerability could be exploited through a XSS (Cross-Site-Scripting) attack.
Ultimately, the attacker could take complete control of the victims web-browser.
In a successful attack, the malicious script would be executed with the authenticated user permissions.

Impact:

Generally, by exploiting this kind of vulnerability, it might be possible to achieve possible attack vectors to various kinds of attacks such as:

- Session/Cookie theft
- Account Hijacking
- Identity theft
- Accessing confidential resources
- Accessing pay content
- Account Denial of service

Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the $_GET['address'], $_GET['relativ_base_dir'], $_GET['Pays'], $_GET['Ville'], $_GET['CP'], $_GET['Poids'], $_GET['Action'] and $_GET['num'] input arguments should be properly sanitized for HTML and following ECMAS usage.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.
According to the developer, this issues are not present in the latest release (1.5), which is, at the moment, only available for developers, for testing purposes.

External References:

http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
http://en.wikipedia.org/wiki/Cross-site_scripting
http://en.wikipedia.org/wiki/Code_injection