Path Injection in Simple PHP Blog 0.8.1

Title: Path Injection in Simple PHP Blog 0.8.1
Release Date: 2013/02/25
Vulnerable Application: Simple PHP Blog 0.8.1
Type: Path Injection
Level: High (Low/High/Critical)
CVSS: 4.9 (Av:N/AC:L/Au:S/C:P/I:P/A:C)

Dognædis Ref.: DGS-SEC-15
CVE Ref.: CVE-2013-2286
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): RAmaro - CodeV Team
Contact: irt@dognaedis.com

Overview:

Simplephpblog.com will give all users a venue to gather basic and complex information about the language, its uses, and recent updates or upgrades made. It will provide developers and people who are not very technical savvy assistance and support to better understand and use the language. The site is committed to provide a helping hand to everyone including tips and suggestions on choosing the web host for your website. It will provide data from the original PHP 5.0 to the PHP 5.4 that comes with all the bells and whistles there is in a modern web language. Articles and discussions on the PHP language, the PHP ecosystem and collaboration will be posted to give users the power to maximize its use when they do use it for their websites.

Scope:

File: <app_root>/zip.php
Vulnerable Argument(s): $directory
Code:

```
line 47: if ($handle = opendir($directory))
```

Proof(s) of Concept:

```
<app_root>/zip.php?dirs=config,content
```

Description:

The referred vulnerabilities could be exploited through Path Injection attacks.
By performing this kind of attack, it is possible to inject files into a non expected location.

Impact:

Generally, by exploiting this kind of vulnerability, it might be possible to achieve possible attack vectors to various kinds of attacks such as:
- Code injection
- Server Denial of service

Resolution:

The path to the directory should be validated as an being part of the files tree of the application.

Official Solution:

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

External References:

https://www.owasp.org/index.php/Relative_Path_Traversal
https://www.owasp.org/index.php/Path_Traversal
https://www.owasp.org/index.php/Resource_Injection