Abysssec Research

1) Advisory information

Title	**: Zenphoto config update and command execute Vulnerability**
Affected	**: Zenphoto <= 1.3**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.zenphoto.org**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **Remote Config Update**
2- **Remote Command Execute**

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying application/server.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Remote Config Update:

```
----------
Line 25 :
---------
Setup Config file CONFIGFILE :
define('CONFIGFILE',dirname(dirname(__FILE__)).'/'.DATA_FOLDER.'/zp-config.php');
```

Setup.php is looks secure in first view and if zp-Config.php be available, MySQL can connect to server, setup.php will read administrator Table from MySQL database & question User/Pass from you.

```
-----------
line 128 :
----------
Update Config File with poor Security check :
if (isset($_POST['mysql'])) { //try to update the zp-config file
        setupLog(gettext("MySQL POST handling"));
        $updatezp_config = true;
        if (isset($_POST['mysql_user'])) {
                updateItem('mysql_user', $_POST['mysql_user']);
        }
        if (isset($_POST['mysql_pass'])) {
                updateItem('mysql_pass', $_POST['mysql_pass']);
        }
        if (isset($_POST['mysql_host'])) {
                updateItem('mysql_host', $_POST['mysql_host']);
        }
        if (isset($_POST['mysql_database'])) {
                updateItem('mysql_database', $_POST['mysql_database']);
        }
        if (isset($_POST['mysql_prefix'])) {
                updateItem('mysql_prefix', $_POST['mysql_prefix']);
        }
}
```

And then write Config file without check:

```
if ($updatezp_config) {
        @chmod(CONFIGFILE, 0666 & $chmod);
        if (is_writeable(CONFIGFILE)) {
                if ($handle = fopen(CONFIGFILE, 'w')) {
                        if (fwrite($handle, $zp_cfg)) {
                                setupLog(gettext("Updated zp-config.php"));
```

```
                                        $base = true;
                                }
                        }
                        fclose($handle);
                }
}
```

After changing admin password you can Edit themes from themes Tab and Upload your malignant PHP file and execute your own commands.