security-assessment.com

Vulnerability Advisory

Name	Wordpress Authenticated Arbitrary File Upload vulnerability
Vendor Website	WordPress (www.wordpress.org)
Date Released	21/06/2012
Affected Software	WordPress <= 3.3.2
Researcher	Denis Andzakovic (denis.andzakovic@security-assessment.com)

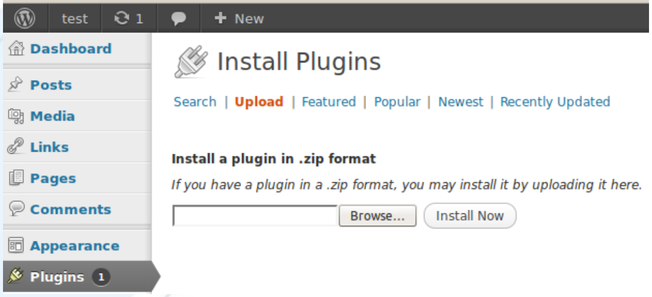
Description

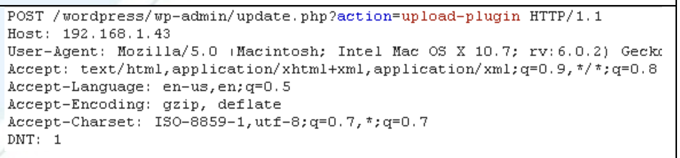
Security-Assessment.com has discovered that the plugin upload function within the WordPress administrative interface is vulnerable to an un-validated file upload attack. Whilst the media upload functionality successfully validates the uploaded file and rejects those not matching the correct extension, the plugin upload functionality does not. This allows an authenticated WordPress administrative user to upload arbitrary files, including a malicious PHP script.

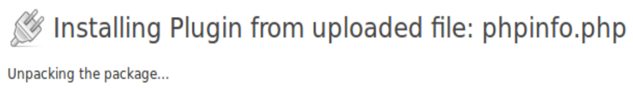
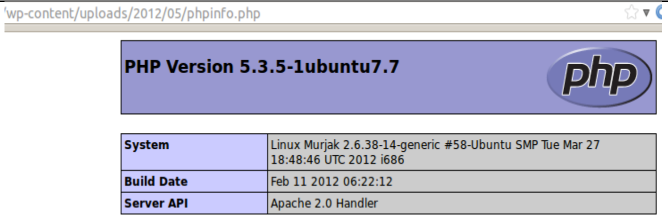
Exploitation

Exploitation of this vulnerability requires a malicious user with access to the admin panel to use the '**/wp-admin/plugin-install.php?tab=upload**' page to upload a malicious file. Upon clicking upload, the page displays an 'installing plugin' message that loops indefinitely. Regardless of installation status and prior to the user being prompted for SFTP credentials, the file is uploaded into the '**/wp-content/uploads/**' directory. At this point, the malicious user can simply browse to '**http://<vulnerablesite>/wp-content/uploads/<year>/<month>/<uploadedfile>**'. A PHP shell can be uploaded in this manner in order to gain arbitrary remote command execution.

Exploit steps

Step	**Summary**	**Screenshot**
'Upload' page	A malicious user browses to the upload section of the plugin install page, they click 'browse', select their PHP file and click 'Install Now'.	 test 1 + New Dashboard Posts Media Links Pages Comments Appearance Plugins 1 Browse... Install Now Install Plugins Search | **Upload** | Featured | Popular | Newest | Recently Updated **Install a plugin in .zip format** *If you have a plugin in a .zip format, you may install it by uploading it here.*

Upload POST request	The POST request containing the arbitrary PHP file upload	
		`POST /wordpress/wp-admin/update.php?action=upload-plugin HTTP/1.1`
		`Host: 192.168.1.43`
		`User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:6.0.2) Gecko`
		`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`
		`Accept-Language: en-us,en;q=0.5`
		`Accept-Encoding: gzip, deflate`
		`Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7`
		`DNT: 1`

'Loading' page	The page returned to the user after clicking 'Install Now'. This loops indefinitely and can simply be stopped.	 Installing Plugin from uploaded file: phpinfo.php Unpacking the package...
PHP Command execution	PHP Command execution after browsing to the uploaded file.	 'wp-content/uploads/2012/05/phpinfo.php **PHP Version 5.3.5-1ubuntu7.7** **System**: Linux Murjak 2.6.38-14-generic #58-Ubuntu SMP Tue Mar 27 18:48:46 UTC 2012 i686 **Build Date**: Feb 11 2012 06:22:12 **Server API**: Apache 2.0 Handler

Work Around

Modify the web server configuration to disable the execution of PHP within the uploads directory.

Apache Example:

In the VirtualHost directive, at the following:

```
<Directory /full/path/to/uploads/directory>
    php_flag engine off
</Directory>
```

Disclosure Timeline

31-05-2012	Initial vulnerability report sent to WordPress Security Team.
07-06-2012	Follow up email sent to WordPress Security Team.
08-06-2012	Emails between SA and WordPress Security Team. WST asserts that this is not a vulnerability and that "we just have to trust that the administrator isn't uploading malicious PHP".
21-06-2012	Release of this advisory.

About Security-Assessment.com

Security-Assessment.com is Australasia’s leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.