Image resizing utility on zero-day WordPress error

Hackers are exploiting the error of the image resizing utility TimThumb, which is widely used in WordPress blogging platform. Some fixes have been included in the latest version of TimThumb.

Hackers are exploiting the error of the image resizing utility TimThumb, which is widely used in WordPress blogging platform. Some fixes have been included in the latest version of TimThumb.

Feedjit CEO Mark Maunder discovered the problem when his blog started downloading advertising content (before that his blog did not have ads). He traced the cause to the problem with the "timthumb.php" library, used in the theme he bought for his blog.

TimThumb "is inherently unsafe" because it writes files to a folder when it loads images and resizes images, and people who visit the website can access that folder, Maunder wrote. An attacker can damage the website by "tricking" TimThumb to load a malicious PHP file and put it into the WordPress directory. Then, if the attacker uses the web browser to access the file, the code will be executed.

Mr. Maunder explained how to disable the ability to load images from TimThumb's external websites, but the surest way to prevent the problem is to remove TimThumb or restrict its access to other websites. . Besides, users should update to the latest version of TimThumb.

Mr. Ben Gillbanks - developer TimThumb - was the first to comment on Mr. Maunder's blog post. Mr. Gillbanks expressed his regret and hoped no one would encounter anything too bad for their website because of his

mistake.

Mr. Gillbanks recommends that people use the latest version of TimThumb to avoid being exploited.