链滴

关于 wordpress WP_Image_Editor_Imagick 指令注入漏洞

作者：retozero

原文链接：https://ld246.com/article/1479374352185

来源网站：链滴

<h2 id="说明">说明</h2>
近日阿里云的云盾安骑士提醒 wordpress 存在图片处理的安全漏洞。
<h2 id="漏洞描述">漏洞描述</h2>
漏洞名称：wordpress WP_Image_Editor_Imagick 指令注入漏洞
补丁编号：7813220
补丁文件：/var/www/html/wp-includes/media.php
补丁来源：云盾自研
更新时间：2016-09-18 07:55:13
漏洞描述：该修复方案为临时修复方案，可能存在兼容风险，为了防止 WP Image_Editor_Imagick 扩展的指令注入风险，将 wordpress 的默认图片处理库优先顺序改为 GD 先，用户可在/wp-includes/media.php 的_wp_image_editor_choose()函数中看到被修改的部分。
<blockquote>
【注意：该补丁为云盾自研代码修复方案，云盾会根据您当前代码是否符合云盾自研的修复模式行检测，如果您自行采取了底层/框架统一修复、或者使用了其他的修复方案，可能会导致您虽然已修复了改漏洞，云盾依然报告存在漏洞，遇到该情况可选择忽略该漏洞提示】
</blockquote>
<h2 id="解决方案">解决方案</h2>
根据漏洞描述，去 wordpress 安装目录下/wp-includes/media.php 文件中搜索 ‘WP_Image_ditor_GD’ 关键字，并将下面一行代码
<pre><code class="language-php highlight-chroma">
$implementations = apply_filters('wp_image_editors', array('WP_Image Editor_Imagick' , 'W_Image_Editor_GD'))

</code></pre>
修改为:
<pre><code class="language-php highlight-chroma">
$implementations = apply_filters('wp_image_editors', array('WP_Image Editor_GD' ,'WP_Image_Editor_Imagick'))

</code></pre>
即将 wordpress 的默认图片处理库优先顺序改为 GD 优先
然后在服务器安全(安骑士)控制台中，点击漏洞列表中此漏洞后边的"验证一下"，若状态变为文已修改，即修复完成。