预警编号：YJ-2018007

恒安嘉新

关于 PHP GD Graphics Library

存在拒绝服务漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 2 月 2 日

1 漏洞描述

近期，互联网爆出 PHP GD Graphics Library 存在拒绝服务漏洞（CVE-2018-5711）。综合利用上述漏洞，攻击者可以构造恶意 GIF 文件，远程调用 PHP 函数形成无限循环的方式发起拒绝服务攻击。该漏洞危害程度为高危(High)。

2 影响范围

PHP 5 < 5.6.33 版本

PHP 7.0 < 7.0.27 版本

PHP 7.1 < 7.1.13 版本

PHP 7.2 < 7.2.1 版本

3 漏洞原理

PHP（超文本预处理器）是一种通用开源脚本语言。GD Graphics Library（又名 libgd 或 libgd2）是一个开源的用于动态创建图像的库，它支持创建图表、图形和缩略图等，广泛应用于 PHP 语言的开发。

该漏洞触发的前提条件为受影响版本的 PHP，并且使用了 libgd 库，漏洞文件存在于 ext/gd/libgd/gd_gif_in.c。在“LWZReadByte_”函数存在一个循环（while-loop），该循环里“GetCode_”函数会调用 GetDataBlock 来读取 GIF 图片中的数据，但由于“GetCode_”函数未能正确处理 int 到 unsigned

char 的类型转换，导致 PHP 在解析特定 GIF 文件调用 PHP 函数 imagecreatefromgif 或 imagecreatefromstring 时出现死循环，从而导致服务器计算资源大量消耗，直至崩溃宕机。该漏洞允许远程攻击者利用该漏洞导致拒绝服务攻击。

4 修复建议

建议广大用户升级到最新版本，厂商已发布最新版本已修复该漏洞。

最新版本下载链接：http://php.net/downloads.php