预警编号：YJ-2017029

恒安嘉新

关于 Zeta Components Mail 存在

远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 11 月 15 日

1 漏洞描述

近期，互联网爆出 Zeta Components Mail 存在的远程代码执行漏洞（CVE-2017-15806），远程攻击者利用漏洞可通过构造恶意邮件在目标系统上执行任意代码。漏洞细节和利用代码已公开，近期被不法分子利用进行攻击尝试的可能性较大。漏洞危害程度为高危(High)。

2 影响范围

漏洞影响 Mail 1.8.1 及之前的版本

3 漏洞原理

Zeta Components 是一个基于 PHP 5 实现的高质量的、通用的应用程序开发库，该项目曾于 2010 年 5 月加入 Apache Incubator，但在 2012 年 4 月退出了 Apache 软件基金会。

安全研究人员在 Zeta Components 的 Mail 库中发现一个远程代码执行（RCE）漏洞，该漏洞存在于 Mail 库中，ezcMailMtaTransport 类中的 send 函数。 send() 函数调用 PHP mail() 来发送邮件，通常 PHP 会使用 sendmail 作为默认的 MTA，当 mail()函数被调用的时候，它的第五个参数$additionalParameters 将允许向 sendmail 传入额外的参数。在 Mail 库中，给$additionalParameters 赋值的代码为：$additionalParameters = "-f{$mail->returnPath->email}”，如果攻击者通过伪造邮箱地址（例如： ‘attacker@outlook.

com -X/var/www/html/cache/exploit.php’ ），再将 payload 放在邮件正文中，sendmail 就会将日志写入/var/www/html/cache/exploit.php 文件中（向 sendmail 传入-Xlogfile，会写入日志到 logfile），最终导致该文件会包含邮件正文中的 payload， 通过远程访问 #域名#/cache/exploit.php 就能够执行 payload。

该漏洞利用需要满足三个条件：

1、使用 ezcMailMtaTransport；

2、使用 sendmail 作为 MTA；

3、对 ezcMailAddress 未做正确转义。

4 修复建议

厂商已发布修复补丁，建议用户升级 Mail 到 1.8.2：

https://github.com/zetacomponents/Mail