预警编号：YJ-2018008

恒安嘉新

关于 Exim SMTP Mail Server

存在缓冲区溢出漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 3 月 8 日

1 漏洞描述

近期，互联网爆出 Exim SMTP Mail Server 缓冲区溢出漏洞（CVE-2018-6789）。攻击者可利用该漏洞在受影响的应用程序上下文中，通过堆溢出实现代码的执行，若攻击尝试失败仍可导致拒绝服务条件。目前，漏洞利用代码尚未公开，厂商已发布漏洞修复版本。该漏洞危害程度为高危(High)。

2 影响范围

漏洞影响 Exim 4.90.1 之前的版本。

据互联网的 Exim SMTP Mail Server 的资产普查数据显示，在全球的分布情况中，美国占比最多（51.32%），其次是德国（4.51%）和荷兰（4.5%），而在我国境内的分布较少（2.01%）。

3 漏洞原理

Exim 是一个 MTA（Mail Transfer Agent，邮件传输代理）服务器软件，该软件基于 GPL 协议开发，是一款开源软件。该软件主要运行于类 UNIX 系统。通常该软件会与 Dovecot 或 Courier 等软件搭配使用。

该漏洞是源于 Exim 4.90.1 之前版本中 SMTP 侦听器'base64d()'解码函数在发送 handcrafted 消息时存在缓冲区溢出漏洞，由于 Exim 未能充分检查用户提供的数据。攻击者可利用该漏洞绕过了 ASLR、PIE、NX 等系统通用系统缓解措施，在受影响的应用程序上下文中执行任意代码，若攻击尝试失败仍可导致拒

绝服务。

4 修复建议

建议广大用户及时更新到漏洞修复后版本，厂商已发布最新版本已修复该漏洞。

最新版本下载链接：https://www.exim.org/mirmon/ftp_mirrors.html