信息安全风险预警

各信息安全重点单位：

近期爆出 OpenSSL 1.0.1 至 1.0.1f 版本，以及 1.0.2 beta 版本存在“Heartbleed”漏洞（编号：CVE-2014-0160）。OpenSSL 主要用于实现互联网上隐私信息的传输，该漏洞使攻击者能够获取通过 OpenSSL 加密传输的隐私数据，可能包含证书私钥、用户名与密码、聊天消息、电子邮件以及重要的商业文档和通信等。

请各单位检查信息系统，若发现有此漏洞请尽快修复，消除隐患。

修复建议如下：

1) 尽快升级为 OpenSSL 1.0.1g 版本。该补丁本质上是一项边界检查，旨在利用 SSL3 结构中的正确长度记录描述输入的 HeartbeatMessage。
2) 补丁细节：https://www.openssl.org/news/secadv_20140407.txt。
3) 补丁可在 https://www.openssl.org/source/下载。

上海市网络与信息安全应急管理事务中心

2014-04-15