安全相关事件

12306 密码泄露事件

时间：2014 年 12 月

事件描述：大量 12306 用户数据及明文密码被泄露到互联网上。12306 网站方面否认是从该网站泄露，而有猜测指这批泄露密码是因为部分抢票工具被盗取数据库并且撞库得出。

索尼影业遭黑客入侵事件

时间：2014 年 11 月

事件描述：一个名为 “Guardians of Peace” （“GOP”) 的黑客组织为了胁迫索尼影业取消讽刺喜剧电影「刺杀金正恩」的上映，入侵并泄露了大量该公司内部资料，包括雇员及家人的信息、员工间的内部邮件记录、员工工资以及当时尚未上映的电影拷贝。美国相关情报官员指出该网络攻击获得超县政府的资助，但也有消息称是索尼影业内部有员工故意泄露相关信息。

POODLE 攻击

时间： 2014 年 10 月

事件描述：POODLE 指 Padding Oracle On Downgraded Legacy Encryption。是一种针对 SSL 3 安全传输加密算法的 padding oracle 攻击。攻击者可以通过中间人的攻击手法截获 SSL 通信中的部分信息的明文。对应的 CVE ID 为 CVE-2014-3566, CVE-2014-8730 。

Shellshock

时间：2014 年 9 月

事件描述：是指一系列在 Bash shell 上发现的安全缺陷。攻击者可以通过这些缺陷调用目标机器上的 bash 终端并执行任意代码。因为网络上存在大量使用 Unix 家族和 bash 终端的服务器，所以攻击者可以通过发起请求和进行 cgi 注入等方式来获取目标主机的权限。 对应的 CVE ID 为 CVE-2014-6271 。（修复耗时周期很长很长的衣蛾漏洞）

Heartbleed

时间： 2014 年 4 月

事件描述：heartbleed 是指一个在 OpenSSL 加密算法库中发现的安全漏洞（数据边界检查的缺失）。攻击者可以可以通过溢出攻击（buffer over-read）的方式来绕过 OpenSSL 的加密算法，获得明文内容。因为 OpenSSL 被广泛用作实现 TLS （传输层加密协议），所以该漏洞影响了大量使用了 OpenSSL 加密算法生成 HTTPS 证书的网站。同时也暴露出 OpenSSL 项目组存在多年的问题，并由此衍生了 LibreSSL 等项目。该事件对应的 CVE ID 为 CVE-2014-0160 。