2亿网民网银密码或中招最危险漏洞 多家中国互联网企业表示已修复

“心脏出血”修复就安全了吗

4月8日外媒爆出，研究人员发现OpenSSL漏洞遍及全球互联网公司，并为其起了个形象的名字“心脏出血”，中国超过3万台主机受波及，4月7日、4月8日期间，共计约2亿网友访问了存在漏洞的网站。国内网站和安全厂商技术人员为检查、抢修彻夜未眠。截至9日，有超30%的主机已经修复，“大站”纷纷表示安全，但技术人士称，消费者敏感信息是否泄露还有待日后观察。

□事件

OpenSSL漏洞曝光

4月8日，OpenSSL的大漏洞曝光，外国黑客将其命名为"heartbleed"，用最致命的内伤“心脏出血”描述事件的严重性。该漏洞是由Codenomicon和谷歌安全部门的研究人员独立发现的。不过据外媒报道，为了将影响降到最低，研究人员已经与OpenSSL团队和其他关键的内部人士展开了合作，在公布该问题前就已经准备好修复方案。

OpenSSL是为网络通信提供安全及数据完整性的一种安全协议，囊括了主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议，各大网银、在线支付、电商网站、门户网站、电子邮件等重要网站上广泛使用。知道创宇网站安全部总监余弦将OpenSSL形容为“互联网上销量最大的门锁”。此次爆出的这个漏洞，则让特定版本的OpenSSL成为无需钥匙即可开启的废锁，入侵者每次可以翻检户主的64K信息，只要有足够的耐心和时间，他可以翻检足够多的数据，拼凑出户主的银行密码、私信等敏感数据。

“简单识别网站应用是否采用SSL加密，只需要看浏览器地址栏是http，还是https，后者就是用SSL加密的。通常是非常关键的网络服务，比如邮箱、支付、银行。”金山毒霸安全专家李铁军说。

“有这样千载难逢的机会，黑客们是舍不得睡觉的。他们会想尽办法多获取一些服务器上的信息。”360公司技术副总裁谭晓生说。

□影响

互联网安全大地震

“这是近两年来最严重的一次网络安全危机。”360公司技术副总裁谭晓生评价，在以https开头的网站中，初步评估有不少于30%的网站中招，其中包括大家最常用的购物、网银、社交、门户等知名网站，而在手机APP的网银客户端中，则有至少50%存在风险。

据南京翰海源信息技术有限公司创始人方兴介绍，通俗来讲，通过这个漏洞，可以泄露以下四方面内容：一是私钥，所有https站点的加密内容全能破解；二是网站用户密码，用户资产如网银隐私数据被盗取；三是服务器配置和源码，服务器可以被攻破；四是服务器挂掉不能提供服务。

一位安全行业人士透露，他在某著名电商网站上用这个漏洞尝试读取数据，在读取200次后，获得了40多个用户名、7个密码，用这些密码，他成功地登录了该网站。

9日下午，来自知道创宇ZoomEye网络空间搜索引擎的监控显示，国内有22611台主机受影响，而前天这个数字是33303，可以看到情况正在好转，超过30%的主机已经修复。

“漏洞被挖掘出来以后，带来的危害并不会非常快地显现。”瑞星安全专家唐威告诉记者，现阶段企业层面能做的也是对使用的OpenSSL进行排查和升级。

不过，9日也有业内人士称，这个漏洞其实并没那么可怕，因为这是一个旧版本OpenSSL的安全漏洞，开发者把服务器程序升级到OpenSSL1.0.1g就可以解决。

□回应

银行银联支付不受影响

对于OpenSSL的漏洞，有传言称即便是银行网上支付、U盾、银联支付也都并不安全。不过，业内人士9日向记者坦言，该漏洞对银行网上支付、银行U盾使用及银联的影响几乎为零。

中国金融认证中心应用开发部总经理林峰表示，OpenSSL的这个漏洞是由于代码实现不严谨造成的。这个漏洞存在于OpenSSL1.0.1系列版本中，之前的OpenSSL版本不受影响。天猫、淘宝使用的正是这个系列的版本，所以可以窃取到内存中的数据。

“如果银行使用了带有该漏洞的OpenSSL开源软件版本，会有一定的影响。但是这个漏洞只是窃取内存中的数据，银行的用户密码还有一重加密保护，一般不会在SSL服务器解密，所以也就很难拿到银行用户的密码。”

林峰还表示，其实这个OpenSSL的漏洞和U盾的安全性没有什么联系，因为用户的交易敏感信息是通过USB接口送入U盾后，在U盾内部进行加密和数字签名运算，SSL协议是对U盾加密签名后的数据再进行一次传输层的加密。这次OpenSSL的漏洞对U盾没有影响。

此外，中国银联相关负责人9日也回应称，银联核心跨行交易系统运营基于专用网络，与漏洞事件无关。该负责人称，“银联在线支付”等基于互联网的创新业务系统并未使用OpenSSL技术，对于个别外围供应商可能存在的OpenSSL漏洞，银联已通过主动排查，在乌云网等技术人士公开漏洞事件前就已协调供应商消除了隐患，持卡人可以放心使用。

微软百度称未受影响

9日，微软中国方面向记者回应称，没有任何微软产品受到此漏洞的影响。OpenSSL是开源用以实现SSL协议的产品，微软并没有在旗下产品和服务中使用此开源的解决方案。据悉，多数商业公司使用的SSL加密都是付费的，与本次暴露出漏洞的OpenSSL关系不大。

百度方面也表示，百度钱包不受影响。电商当当网表示，当当网固有的账户体系非常安全，消费者可放心购物。

盛大方面表示，盛大通行证的认证主要是通过硬件加密等方式来使用https协议，目前已经和供应商确认过，一方面所使用的OpenSSL版本不是会受影响，另一方面针对有可能出现的安全隐患，已在第一时间通过升级进行了处理。

阿里京东回应已修复

9日早上，此次漏洞事件引发最多泄密担忧的阿里系急忙表示漏洞已经修复。阿里安全回应称，关于OpenSSL某些版本存在基于基础协议的通用漏洞，阿里各网站已经在第一时间进行了修复处理，目前已经处理完毕，包括淘宝、天猫、支付宝等各大网站都确认可以放心使用。其中淘宝方面还透露，从目前监控的情况来看，未发现账户异常。

京东则表示，已于9日完成了修补处理，避免了这次漏洞的侵袭。

腾讯9日早上也发声明称，腾讯已在第一时间进行处理，目前相关的产品业务如邮箱、财付通、QQ、微信等都已经修复完毕。

网易邮箱方面告诉记者，乌云报告提到的网易邮箱OpenSSL漏洞，经过网易邮箱查证，所列域名都是指向了CDN(内容分发网络)服务，收到报告后网易邮箱第一时间反馈给CDN服务商，当晚已经修复。

此外，全球互联网巨头雅虎、谷歌和Facebook也纷纷表示已修复漏洞。谷歌表示：“我们已经评估了SSL漏洞，并且给谷歌的关键服务打上了补丁。”

□消费者应对

网站修复漏洞后用户需修改密码

360公司技术副总裁谭晓生建议，在4月7日和8日两天登录过存在漏洞的网站的网友，首先需要确认曾经登录的网站是否已经进行了升级修复，可看该网站是否发布相关的公告，也可通过360网站卫士推出的OpenSSL漏洞在线检查工具，输入网址检测网站是否存在该漏洞。如果相关网站已完成了修复，则用户需要将使用过的用户名、密码等个人信息进行修改；如果登录过的网站仍然未能完成修复，“那很遗憾，用户只有坐等对方修复。”

金山毒霸安全专家李铁军表示，对重要服务，要尽可能开通手机验证或动态密码，比如支付宝、邮箱等。

“针对OpenSSL漏洞，黑客的攻击方式是不断发动数据包攻击，每次攻击能够从服务器内存上得到大小为64K的数据，不过获得的数据是零散无序的，黑客想要获得真正有用的信息，需要把累计获得的数据进行整理分析，这需要一个时间过程，因此，在这两天内及时完成密码修改，就不会有太大的问题。”谭晓生提醒说，不过，即便网站完成修复，也并不意味着天下太平了，未来是否有新的危险还不得而知。

此外，在网站漏洞修复前，不要网购或网上支付，以免受到损失。一个密码的使用时间不宜过长，超过3个月就该换掉了。

什么是SSL?

SSL是一种流行的加密技术，可以保护用户通过互联网传输的隐私信息。网站采用此加密技术后，第三方无法读取你与该网站之间的任何通讯信息。在后台，通过SSL加密的数据只有接收者才能解密。

SSL最早在1994年由网景推出，1990年代以来已经被所有主流浏览器采纳。

什么是“心脏出血”漏洞?

SSL标准包含一个心跳选项，允许SSL连接一端的电脑发出一条简短的信息，确认另一端的电脑仍然在线，并获取反馈。研究人员发现，可以通过巧妙的手段发出恶意心跳信息，欺骗另一端的电脑泄露机密信息。受影响的电脑可能会因此而被骗，并发送服务器内存中的信息。

谁发现的这个问题?

该漏洞是由Codenomicon和谷歌安全部门的研究人员独立发现的。为了将影响降到最低，研究人员已经与OpenSSL团队和其他关键的内部人士展开了合作，在公布该问题前就已经准备好修复方案。

谁能利用“心脏出血”漏洞?

“对于了解这项漏洞的人，要对其加以利用并不困难。”普林斯顿大学计算机科学家菲尔腾说。利用这项漏洞的软件在网上有很多，虽然这些软件并不像iPad应用那么容易使用，但任何拥有基本编程技能的人都能学会它的使用方法。

当然，这项漏洞对情报机构的价值或许最大，他们拥有足够的基础设施来对用户流量展开大规模拦截。

(据京华时报)