热线:96777 E-mail:xdkb@kuaibao.net 现代快报
责编:王娟 美编:江佳锲 组版:滕爱花 2014.4.10 星期四

全球互联网“心脏出血”

一句话科普:OpenSSL就是互联网上销量最大的门锁。不过最新曝出的这个漏洞，则让它成为无需钥匙即可开启的废锁,虽然这把废锁被打开的概率不高,但保险起见,请修改密码。

2014年4月8日,必将永载于互联网史册。这一天,互联网世界发生两件大事:一、微软正式宣布XP停止服务退役;二、OpenSSL的超级大漏洞曝光。

很多普通人更关心第一件事,因为与自己切身相关。但事实上,第二件事,才是真正的大事件。

这个漏洞影响了多少网站,数字仍在评估当中,但放眼放去,我们经常访问的支付宝、淘宝、微信公众号、YY语音、陌陌、雅虎邮件、网银等各种网站,基本上都出了问题。

这一漏洞一旦被恶意利用,意味着用户登录这些电商、网银的账户、密码等关键信息都有可能泄露,造成财产损失。

而在国外,受到波及的网站也数不胜数,就连大名鼎鼎的NASA(美国航空航天局)也已宣布,用户数据库遭泄露。

这个漏洞被曝光的黑客命名为“heartbleed”,意思是“心脏出血”——代表着最致命的内伤,这是一个极为贴切的表述。

这一夜,互联网门户大开

网络基础安全协议曝出大漏洞

4月8日，网络安全协议OpenSLL被曝出存在安全漏洞,该协议常用于电商、网银等安全性极高的网站。

该漏洞是由安全公司Codenomicon和谷歌安全工程师发现的。为了将影响降到最低,该研究人员已经与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。

程序员Sean Cassidy在自己的博客上详细描述了这个漏洞的机制。他披露,**OpenSSL的源代码中存在一个漏洞,可以让攻击者获得服务器上64K内存中的数据内容。这部分数据中,可能存有安全证书、用户名与密码、聊天工具的消息、电子邮件以及重要的商业文档等数据。**

OpenSSL是目前互联网上应用最广泛的安全传输方法。可以说,它是互联网上销量最大的门锁。而Sean曝出的这个漏洞,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;假如户主是个开商店的或开银行的,那么在他这里买东西、存钱的用户,其个人最敏感的数据也可能被入侵者获取。发现者们给这个漏洞起了个形象的名字:heartbleed,“心脏出血”。这一夜,互联网的安全核心,开始滴血。

真相是这样的

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。当用户访问Gmail.com等安全网站时,就会在URL地址旁看到一个“锁”,表明你在该网站上的通讯信息都被加密。

这个“锁”表明,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。如果不法分子监听用户的对话,也只能看到一串随机字符串，而无法了解电子邮件、Facebook帖子、信用卡账号或其他隐私信息的具体内容。

SSL最早在1994年由网景推出,已经被所有主流浏览器采纳。最近几年,很多大型网络服务都已经默认利用这项技术加密数据。如今,谷歌、雅虎和Facebook都在使用SSL对其网站和网络服务进行加密。

谁能利用漏洞?

“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,任何拥有基本编程技能的人都能学会它的使用方法。

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。我们知道,美国国家安全局(以下简称“NSA”)已经可以进入到互联网的骨干网中。用户或许认为,Gmail和Facebook等网站上的SSL加密技术可以保护他们不受监听,但NSA 却可以借助“心脏出血”漏洞获取解密通讯信息的私钥。

虽然现在还不能确定，但如果NSA在“心脏出血”漏洞公之于众前就已经发现这一漏洞,也并不出人意料。

什么是“心脏出血”漏洞

多数SSL加密的网站都使用名为OpenSSL的开源软件包。

4月8日，研究人员宣布这款软件存在严重漏洞，可能导致用户的通讯信息暴露给监听者。

据悉,OpenSSL大约两年前就已经存在这一缺陷。

“心脏出血”漏洞的工作原理: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。

有多少网站受到影响?

目前还没有具体的统计数据,但发现该漏洞的研究人员指出,当今最热门的两大网络服务器Apache和nginx都使用OpenSSL。总体来看,这两种服务器约占全球网站总数的三分之二。

雅虎:“我们的团队已经在雅虎的主要资产中(包括雅虎主页、雅虎搜索、雅虎电邮、雅虎财经、雅虎体育、雅虎美食、雅虎科技、Flickr和Tumblr)成功部署适当的修复措施。”

谷歌:“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。”Facebook称,在该漏洞公开时,该公司已经解决了这一问题。

微软发言人也表示:“我们正在关注OpenSSL问题的报道。如果确实对我们的设备和服务有影响，我们会采取必要措施保护用户。”

这一漏洞,堪称“地震级别”

影响严重:还不知哪些服务器被入侵

“对于一个安全协议来说,这样的安全漏洞是非常严重的。”北京知道创宇信息技术有限公司研究部总监钟晨鸣说。

该漏洞只能从内存中读取64K的数据，而重要信息正好落在这个可读取的64K上的几率并不大，但是攻击者可以不断批量地去获取这最新的64K数据，这样就很大程度上可以得到尽可能多的用户隐私信息。

据南京翰海源信息技术有限公司创始人方兴介绍,**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,用户资产如网银等隐私数据被盗取；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,他成功登录该网站。

更大威胁: 部分涉及机构竟盲目乐观

这一漏洞被曝出后，全球的黑客与安全保卫者们展开了竞赛。黑客在不停地试探各类服务器，试图从漏洞中抓取到尽量多的用户数据；安全保卫者则在尽可能短的时间里升级系统、弥补漏洞,实在来不及实施的则暂时关闭某些服务。

根据知道创宇公司持续在线监测情况来看，并非所有受到该漏洞威胁的公司都认识到了这一危害性，部分涉及机构盲目乐观。有的只是暂停SSL服务,仍继续提高其主要功能,比如微信;有的为规避风险,干脆暂停网站全部服务；还有的没有采取任何措施。

钟晨鸣说，**这个漏洞实际上出现于2012年,至今两年多,谁也不知道是否已经有黑客利用漏洞获取了用户资料；而且由于该漏洞即使被入侵也不会在服务器日志中留下痕迹，所以目前还没有办法确认哪些服务器被入侵,也就没法定位损失、确认泄漏信息,从而通知用户进行补救。**

存在短板:我国网络安全应急能力差

作为国内顶尖的安全专家,方兴指出,此次发现的漏洞事实上是非常简单的一个漏洞,并不是因为算法被攻破,而是由于程序员在设计时没有做长度检查而产生的内在泄露漏洞。“几乎所有程序员都很容易犯的错误,即使微软的高手,开源的精英也容易犯。”程序员的一时疏忽引发了蝴蝶效应，带来了全球网络安全危机。

“SSL是广泛使用的数据传输加密协议,这个漏洞是大地震级别的。”中国计算机学会信息安全专业委员会主任严明说。

分析人士指出，具体受害的用户数字要到后面才能得以统计，当前应动员所有应急机制做出紧急反应，并通报如何尽量减少威胁。建议大型站点需要换证，重新配置一些重要程序和配置里的密码串。国家应急中心直到9日才开始联动。

该中心一名专家坦陈，从2003年,国家应急中心就试图建立漏洞触发的相关应急工作和能力，但是这一领域的工作到现在也不够清晰,需要新的能力架构设计。

我们该怎样自保

怎么办?少用网银 谨防失财

对一般网民来说，如果访问了受影响的网站，用户无法采取任何自保措施。受影响的网站的管理员需要升级软件,才能为用户提供适当的保护。

不过，一旦受影响的网站修复了这一问题，用户便可以通过修改密码来保护自己。攻击者或许已经拦截了用户的密码，但用户无法知道自己的密码是否已被他人窃取。

所以,对于个人用户而言,目前最迫切的就是:改密码。此外,在未确认安全的情况下,尽量少用网银,密切观注你的财务状况。

综合新华社消息