“心脏出血”急救指南

普通人如何应对此次网络安全漏洞威胁?

4月8日,常用于电商、网银等安全性极高网站的网络安全协议OpenSSL被曝出存在安全漏洞,危及全球包括银行、电商在内关键部门和普通用户财产和信息安全。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、密码等关键信息都将泄露。

这一次互联网的“致命内伤”被命名为“心脏出血”,其威胁处于持续发酵之中,为了避免中招,普通人要如何应对?

综合消息

A 领会要点

1

改掉你认为比较重要的一些网站的登录密码,这可能不是特别必要,但是得以防万一啊!

2

对于那些你认为比较重要的网站,不要使用相同的登录密码,任意两个网站的密码都不能重复。不管有没有“心脏出血”漏洞,这都有助于提高你的网络安全。

3

使用密码管理软件,这种软件能生成一组独特的、难以破解的密码,并且帮你记住它们。

4

登录网站时使用双重认证,从你的邮箱开始。

5

严肃认真地对待以上建议,必要时读读相关文章,了解一下密码被盗的可怕后果。

B 实践操作

检查常用网站

目前还不清楚到底有多少互联网站受到了影响以及多少密码已经被盗。但是如果你是Yahoo,OKCupid和Github的用户,最好是趁早换掉你的密码。

一些大型网络公司都正在试图修复这个问题,你可以在https://www.ssllabs.com/ssltest 上查看你常去的网站,如果安全等级以绿色显示,说明该网站已经升级,你可以更改密码了,如果是红色显示,那你还得暂时等着网站升级完毕,否则就算改了新密码也可能被继续盗取。

实际上,就算没有“心脏出血”,你也应该每90天换下你的重要密码。

至少使用5种不同密码

最大的错误是把你所有的密码都设成了同一个,这样只要你的密码在一个网站上被破解,黑客很快会用同一个密码去尝试你别的账户。

比分别记忆每一个站点的不同密码更好的,是按群组记忆。比如可以从5个最基本的群组开始,“银行”“邮件”“社交”“购物”以及“不太常用”。然后可以试着按照字母顺序在每一个群组登录密码最后加上一两个不同的字母。

这样做的好处是,在黑客破解其中某一组密码后,还会给你一些喘息的时间,去改掉其他群组的密码。

使用双重认证

除了更新密码以外,双重认证密码服务也显得更加重要起来。

在许多邮件、银行和社交媒体网站上,登录时系统都会给你发一个即时密码,在每一次登录时都必须输入这个即时密码。

用更强大的密码

什么样的密码最强大?当然是越长越好,最起码有6到8个字母和数字混合。

注意,宠物和家庭姓名是一个糟糕的选择,因为犯罪分子可能已经通过你的facebook掌握了你的个人信息。

还有要记得邮箱密码是极端重要的,因为在登录你邮箱后,黑客可以通过利用“忘记密码”服务来获取你在其他站点的密码。

一个比较好的办法是,可以在设置密码安全问题时故意设置一个和你真实生活不符的错误答案,这样已经了解你个人信息的黑客反而没有办法以真实信息通过这个测试。

怎么记住复杂密码?

虽然把你的密码写下来放在钱包里同样也会面临风险,但把那些难以破解的复杂密码写下来藏在安全的地方,也比为了方便记忆而选择那些容易破解的密码好得多。

而且还有一些好办法来记忆那些难记的密码,比如运用记忆术。可以选择一个短语或者词组,将该词组每一个单词的大写字母开头作为密码。比如“I Left My Heart In San Francisco”可以组合出“ILMHISF”。

注意不要限于那些真实存在于你生活中的表达或者词组,你捏造得越厉害,黑客越难破解。

还有一些人喜欢用密码管理服务来记忆密码,一些安全专家对此事的风险性也有质疑。

不过总的来说,这些都比你简单地把密码设成1234要好得多。

事件追踪

安全漏洞 威胁持续发酵

OpenSSL“心脏出血”漏洞威胁持续发酵,据360漏洞研究实验室最新分析,此漏洞不仅影响以https开头的网站,黑客还可利用此漏洞直接对个人电脑发起攻击。

据360介绍,在全球最大的社交编程及代码托管网站GitHub上,已有黑客晒出利用“心脏出血”漏洞攻击个人电脑客户端的代码。这意味着,即便用户不去登录存在OpenSSL漏洞的网站,当访问被黑客控制或者伪造的https网站时也面临被攻击的风险。

美国安局 否认早就知情

在彭博社11日披露美国国家安全局(NSA)早在两年前就已经知晓这一漏洞,并且借此搜集外国情报后,恐慌情绪进一步蔓延。不过,NSA、白宫和美国国家情报总监办公室均否认了这一报道。

“有关NSA或其他美国政府部门在2014年4月之前便已知晓所谓的‘心脏出血’漏洞的报道,均不属实。”白宫国家安全委员会发言人卡特琳·海登说。

“心脏出血”漏洞还引发了人们对另一个问题的思考:互联网是否应该如此集中地依赖同一款技术来保护数据安全。

C “病因”揭秘

OpenSSL项目 缺人又缺钱

美国《华尔街日报》网络版12日撰文称,“心脏出血”漏洞暴露出OpenSSL的一大软肋:如此重要的项目多年来始终面临着资金和人手不足的窘境,多数工作都要由为数不多的志愿者来完成。

项目团队仅有11人

OpenSSL项目的工作量十分艰巨,但多数工作都仅由4位欧洲程序员以及美国马里兰的1位前军事顾问承担。

团队由11人组成,多数是志愿者,只有一人全职工作,他们每年的预算不到100万美元。“心脏出血”漏洞是一位年轻的德国研究人员的一个无心之举导致的。“该项目人员之少令人震惊。”美国安全公司加密专家肯尼斯·怀特说,“要知道,这可是当今互联网上最为复杂的通讯代码之一。”

OpenSSL项目创立于1998年,目的是提供一组免费的加密工具。经过多年发展后,全世界约有2/3的网络服务器都采用了这一工具。各大网站、网络设备公司和政府机构都利用OpenSSL工具保护个人信息和其他敏感数据。因此,当谷歌和Codenomicon披露黑客可能借助“心脏出血”窃取这类数据后,互联网立刻陷入恐慌。

全职开发者只有一人

OpenSSL只有一名全职开发者——史蒂芬·亨森,这位46岁的英国密码学家拥有数学博士学位。另外两位英国居民和一位德国开发者组成了该项目的管理团队。同事认为亨森工作负荷过大。

OpenSSL项目团队不断改进一种名为SSL或TLS的加密协议,保证黑客无法读取用户发给网站的信息。这种如今被广泛使用的软件的基础代码是埃里克·杨开发的,他目前在EMC旗下的RSA安全部门担任工程师。

OpenSSL团队志愿者杰弗里·索普表示,由于在软件公司的工作非常繁忙,所以分配给该项目的时间很少。他说:“这就像清理下水道,肮脏又复杂,但出问题前一切都会被视为理所当然。”

资金不足令问题恶化

消息人士表示,OpenSSL项目的部分资金来自外界捐助,而资金和人手不足导致漏洞问题进一步恶化,使之在长达两年的时间内都没有被发现。

过去10年间,美国防部前顾问史蒂夫·马奎斯通过名叫“OpenSSL软件基金会”的组织,为该项目筹款、签订咨询合同。“心脏出血”漏洞曝光后,该基金会的捐款额略有提升,但多数仍是5美元和10美元的小额捐款。

美国网络安全公司Qualys表示,已向基金会捐献了少量资金用于安全代码工作。虽然该公司发言人不肯透露具体金额,但却表示,OpenSSL将其列为“主要捐赠者”,表明其“资金严重不足”。