针对电脑用户的安全意识电子月刊

# OUCH!

本期导读

- 什么是Heartbleed?
- 我应该怎么做?
- 谨防网络钓鱼攻击

# 为什么我要关心?

## 概述

4月7日（周一），一个严重的，存在于OpenSSL中的安全漏洞被确认了。 OpenSSL是当下最流行的关于SSL协议的一个实现方式，SSL是整个互联网使用的、一个很重要的安全协议。SSL不仅加密您的在线交流，它还有助于确保您连接到合法的网站，比如当您访问在线商城或网上银行的时候。在这个通讯中，我们将给出非常简单的概述，助您了解该漏洞对您意味着什么和您所能做到的自我保护。

**客座编辑**

Jake Williams(@MalwareJake; malwarejake.blogspot.com)是CSRgroup Computer Security Consultants的首席科学家. 他也是SANS的内存取证(FOR526)和恶意软件逆向工程(FOR610)课程的合著者。

## 什么是 Heartbleed?

该Heartbleed漏洞允许黑客连接到某个网络服务器和获取敏感信息，这些信息可能包括您的登录名和密码。如果攻击者能够获得这样的信息，他们可以使用这些信息来登录到您的使用了相同用户名和密码的任何帐户。虽然该漏洞已经存在了近两年，但直到4月7日它才被发现并公布。 Heartbleed不会影响Windows或Mac电脑；它主要影响您访问的互联网上的网站，如Facebook和Gmail。让普通用户难于理解的是，它并不是影响互联网上的每一个网站，但它确实影响到很多个。您可以使用LastPass网站提供的检查工具（https://lastpass.com/heartbleed/），来检查您使用过的网站是否包含潜在风险。

## 我该怎么做?

有这样几个步骤，您可以用来保护自己。这些步骤不仅可保护您免受Heartbleed漏洞的影响，它们还将有助于保护您免受未来其他攻击的影响:

- 首先，从你最重要的账户着手，如果您已经确认使用过的网站存在该漏洞并且已经进行了修补，请修改这些账户的密码。如果您不能确认该网站是否易受攻击和是否已经修补，不管怎样，也还是修改密码为好。这是一个很好的机会来更新您的密码和改善您的网络安全。
- 确保更新您的密码到安全强度“强”的级别，使用难以猜测的密码。此外，如果该网站支持所谓的两步骤验证，请

## 为什么我要关心?

启用它。这是一个额外的步骤，其有助于提高您的帐户安全性。最后，如果您的密码含有个人问题，我们建议您更改答案。

- 确保您使用单独的、唯一的密码来登录每个网上帐户。这样一来，即使一个网站被攻破，所有的其他帐户将仍然是安全的。不记得您所有的密码？恭喜您，您正在使用高强度的密码。我们强烈建议您利用这个机会，开始使用一个密码管理器，让它存储所有的密码。这是很好的工具，不仅可以简化您的网上步骤，并且有助于更安全的上网。
- 不要忘记您的电子邮件客户端。如果您的电子邮件客户端，如Outlook或苹果邮件，是使用SSL连接到您的邮件服务器，您可能也需要更改这些密码。

保护自己的关键一步是更改您的每个关键账户的密码，并确保您使用的是唯一的，强度大的密码。

## 谨防网络钓鱼攻击

不幸的是，坏人都是机会主义者。他们知道，Heartbleed的消息一直在被报导，包括您在内的好多人都读到了。源于这个逻辑，他们将可能制造一个显示为来自您使用的合法网站（如网上银行或商城）的假电子邮件。他们甚至会假装是安全公司提供的免费工具来检查Heartbleed。这种战术（俗称网络钓鱼）不是新花样。攻击者试图欺骗您点击其链接进入恶意网站或欺骗您打开一个受感染的附件链接。如果您成为这种攻击的牺牲品，您的电脑可能被感染。建议您，如果需要更改密码，只需输入网站的地址（通常称为URL）到您的浏览器地址栏，并在网上更改您的密码。这样一来，您知道您正在连接的是合法网站。

## 相关资源

| | |
|---|---|
| Which Sites Are Vulnerable: | https://lastpass.com/heartbleed/ |
| OUCH! Passwords: | http://www.securingthehuman.org/ouch/2013#may2013 |
| OUCH! Password Managers: | http://www.securingthehuman.org/ouch/2013#october2013 |
| OUCH! Two-Step Verification: | http://www.securingthehuman.org/ouch/2013#august2013 |
| OUCH! Phishing: | http://www.securingthehuman.org/ouch/2013#february2013 |
| Technical Details: | https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105 |



编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：成自豪