April 18, 2014

Help Prevent Future "Heartbleeds"

RISK ADVISORY/INTERNAL AUDIT
BY TROY FINE

SHARE WITH A COLLEAGUE | DOWNLOAD PDF

Recently, a Finnish security firm, Codenomicon, discovered the Heartbleed vulnerability in a variant of SSL (Secure Socket Layer) protocol known as OpenSSL. Web servers and browsers use SSL protocol to help protect data during transfer by creating an encrypted channel for private communications over the Internet. OpenSSL is the most common used data transmission encryption on the internet and the Heartbleed vulnerability allows intruders to circumvent its trusted communication channel and obtain access to sensitive information. In essence, Heartbleed creates an opening in SSL's encryption technology which allows a hacker to steal the public and private keys used for deciphering internet traffic, thus enabling a hacker to steal sensitive data that once was thought to be secure. The vulnerability has existed for two years and exploitation is undetectable.

The discovery of the Heartbleed vulnerability emphasizes the importance of a diligent information security vulnerability and incident management program. Organizations should ensure that they actively monitor all available resources to identify alerts for newly discovered security vulnerabilities and take the action steps recommended to help mitigate critical threats such as Heartbleed. It is critical that organizations are diligent in their monitoring of security alerts and timely in their implementation of the recommended patches/upgrades or security fixes provided by vendors or security resources. Subscribing to available resources, such as United States Computer Emergency Readiness Team (US-CERT) or FBI InfraGard security bulletins, and employing external assessors to perform vulnerability scans on systems and infrastructure on a regular basis is critical in the early identification of security exposures and vulnerabilities. Additionally, developing an effective incident response plan will ensure that organizations are well-equipped to respond to high-risk security incidents with early detection, containment and implementation of swift and efficient resolutions.

The vulnerable versions of OpenSSL are 1.0.0 through 1.0.1f. The most recent version of OpenSSL, 1.0.1g, patches the flaw. Companies that employ web applications containing sensitive information or transmit sensitive data over the internet should investigate their current versions of SSL encryption and determine whether they are using a vulnerable version of OpenSSL. Vendors such as Cisco Systems Inc. and Juniper Networks Inc. have made announcements informing customers that some of their products utilize OpenSSL versions that are vulnerable to Heartbleed attacks. In a customer bulletin, Cisco released all of the devices that are vulnerable to the Heartbleed vulnerability and all of the devices that they were currently investigating. Many of the vendors such as Cisco informed customers that they will release free patches for all of their products that were affected. It is highly recommended that you contact your device manufacturers as soon as possible to determine if these devices contain the Heartbleed vulnerability.

In addition to the adverse effect on companies, many consumers were also potentially adversely affected by Heartbleed. Consumers, who use the internet for online banking, paying bills, social media, and a myriad of other services, should continually check their service providers' websites for press releases or updates on

whether the sites they use were affected. To assist consumers with determining whether or not a website is vulnerable to the Heartbleed bug, Google released a plug-in for their Chrome browser called Chromebleed, which will notify users when the website they are currently on is vulnerable. There are also sites that provide consumers with the ability to test URLs for the Heartbleed bug. Many security experts are advising consumers to change their passwords to all sites that have been affected by the bug; however, they are also suggesting waiting until affected websites have resolved the issue. This is due to the fact that hackers would potentially still have access to a user's credentials if they changed their password while utilizing a website that was still using an unpatched version of Open SSL.

For more information on how Schneider Downs can assist you or your company with securing your network, contact Eric Wright.

This advice is not intended or written to be used for, and it cannot be used for, the purpose of avoiding any federal tax penalties that may be imposed, or for promoting, marketing or recommending to another person, any tax related matter.

SHARE

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.

The Privacy of Consumer Banking Data and the Financial Data Exchange

READ MORE >

Register to receive our weekly newsletter with our most recent columns and insights.

SUBSCRIBE FOR UPDATES

MOST RECENT

The Stages of Wealth

401(K) PLANS, WEALTH MANAGEMENT
BY ALISSA SHAWL | 8.15.2019

Although everyone's situation is different, most people will go through various stages of wealth development throughout their lifetime. Over the ...

READ MORE

MOST POPULAR

Tax Treatment of Deferred Revenue in a Taxable Stock Acquisition

MERGERS AND ACQUISITIONS, TAX
BY GARY SLIMAN | 6.1.2016

The general rule under Internal Revenue Code §451 is that an item of income shall be included in gross income for the taxable year or receipt unless ...

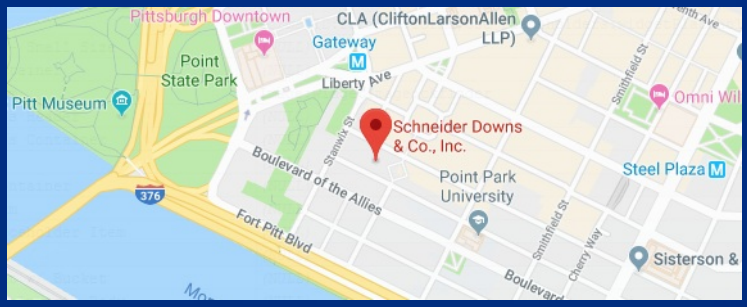
READ MORE

Have a question? Ask us!

We'd love to hear from you. Drop us a note, and we'll respond to you as quickly as possible.

ASK US

CONTACT US



PITTSBURGH
One PPG Place, Suite 1700
Pittsburgh, PA 15222

contactsd@schneiderdowns.com
p:412.261.3644 f:412.261.4876

COLUMBUS
65 East State Street, Suite 2000
Columbus, OH 43215

contactsd@schneiderdowns.com
p:614.621.4060 f:614.621.4062

WASHINGTON, D.C.
1660 International Drive, Suite 600
McLean, VA 22102

contactsd@schneiderdowns.com
p:571.380.9003

PrimeGlobal
An Association of Independent Accounting Firms

FOLLOW US

CLIENT PORTAL

SUBSCRIBE FOR UPDATES

E-mail

SUBMIT

INSIDE PUBLIC ACCOUNTING TOP 100 FIRMS 2018

Schneider Downs is a Top 60 independent Certified Public Accounting (CPA) firm providing accounting, tax, audit and business advisory services to public and private companies, not-for-profit organizations and global companies. We also offer Internal Audit; Technology Consulting; Software Solutions; Personal Financial Services; Retirement Plan Solutions and Corporate Finance Services. Schneider Downs is the 13th largest accounting firm in the Mid-Atlantic region and serves individuals and companies in Pennsylvania (PA), Ohio (OH), West Virginia (WV), New York (NY), Maryland (MD), and additional states in the United States with offices in Pittsburgh, PA and Columbus, OH.