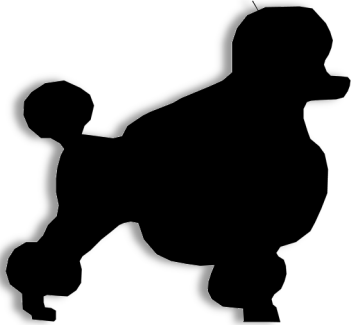


# Security focus

Volume. 4 • Issue. 1  
January 2015



On October 14, 2014, Google discovered a critical vulnerability in Secure Sockets Layer version 3.0 (SSL 3.0) referred to as Padding Oracle On Downgraded Legacy Encryption, also known as “POODLE”. This vulnerability is considered a Man-in-the-Middle (MITM) network attack. This type of attack grants an intruder the ability to access and decrypt secure “cookie” files that are stored on your computer. These files contain website information and user specific settings. By accessing this data, the intruder is able to steal sensitive information or impersonate the user by logging it to their online accounts.

## POODLE Vulnerability: Who’s barking up your network?

### What is Secure Sockets Layer (SSL)?



Secure Sockets Layer (SSL) is a standard security technology that is used to establish an encrypted connection between a web server and web browser to ensure any and all data transmitted between systems is sent securely.

### Companies Taking Action

Companies and services providers immediately began assessing programs and systems that may have supported the use of SSL 3.0 to ensure that the systems or data have been compromised. Furthermore, many have begun taking steps to disable support of SSL 3.0 to prevent future impact. Monterey County Bank has reviewed reports from our service providers to ensure our clients have not been impacted.

### Other Vulnerabilities To Be Aware Of



In April 2014, a security vulnerability referred to as “*The Heartbleed Bug*”, was discovered in a technology called OpenSSL, which is used by a number of websites to create a connection between a browser and the site. OpenSSL is just one kind of SSL and since it’s free to use, up to 60% of all secure websites use OpenSSL.

For additional information: [www.heartbleed.com](http://www.heartbleed.com)



In September 2014, “*Shellshock*” or “*Bash Bug*” was brought to light and similarly compared to Heartbleed to be another programming flaw in older security software. This threat also allows hackers to access vulnerable computers and networks to either steal data or shut down systems.

For additional information: [wikipedia.org/wiki/Shellshock\\_\(software\\_bug\)](http://wikipedia.org/wiki/Shellshock_(software_bug))

### What Should I Do To Ensure I Am Not Impacted?

To avoid service interruptions or potential intrusion, consumers are encouraged to update their internet browsers to the latest versions. Additionally, users should ensure their operating system is running the latest security updates and that their anti-virus software is current.

Although these actions will help strengthen security, consumers should take every precaution to avoid suspicious websites requesting sensitive information or requiring unknown downloads. Do not open links or files sent via email from unfamiliar sources. If you suspect your account has been compromised contact the service company immediately.



### Your BANK working for YOU

If you have any questions or concerns regarding your account please stop by or contact your local branch for additional assistance.

We encourage you to review our website, [www.montereycountybank.com](http://www.montereycountybank.com), for security tips and consumer alerts. If at any time you have questions regarding security or possible fraud, please contact our main office at (831) 649-4600 or you may send an email to [electronic\\_banking@montereycountybank.com](mailto:electronic_banking@montereycountybank.com).

### INTERNET BANKING

The following internet browsers and operating systems have been approved for compatibility with Monterey County Bank’s Internet Banking service.

#### Internet Browsers



**INTERNET EXPLORER**  
Version 8.0 or higher



**SAFARI**  
Version 4.0 or higher (PC)  
Version 5.0 or higher (MAC)



**GOOGLE CHROME**  
Version 9.0 or higher



**MOZILLA FIREFOX**  
Version 3.5 or higher



**OPERA**  
Version 10.0 or higher

#### Operating Systems

##### MICROSOFT WINDOWS

Vista or higher, 32 bit, all editions

##### MAC OS

*NOTE: Internet Banking is not approved for compatibility to access on mobile devices. Accessibility and functionality may be limited.*



Monterey County Bank is the oldest locally owned, locally managed bank servicing the Monterey County for over 35 years with locations in:

#### Monterey

601 Munras Avenue  
Monterey, CA 93940  
(831) 649-4600

#### Carmel Rancho

3785 Via Nona Marie  
Carmel, CA 93923  
(831) 625-4300

#### Pacific Grove

542 Lighthouse Avenue  
Pacific Grove, CA 93950  
(831) 655-4300

#### Salinas

1127 South Main Street  
Salinas, CA 93901  
(831) 422-4600

