FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-16-2014
April 11, 2014

Technology Alert: OpenSSL “Heartbleed” Vulnerability

Summary: The FDIC, as a member of the Federal Financial Institutions Examination Council (FFIEC), is issuing the attached alert advising financial institutions of a material security vulnerability in OpenSSL, a popular cryptographic library used to authenticate Internet services and encrypt sensitive information.

Statement of Applicability to Institutions with Less than $1 Billion in Total Assets: This Financial Institution Letter (FIL) applies to all FDIC-supervised institutions**.**

Suggested Distribution:

FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:

Chief Executive Officer
Chief Information Office
Chief Information Security Officer

Attachment:

OpenSSL “Heartbleed” Vulnerability Alert

Related Topics:

FFIEC IT Examination Handbook
http://ithandbook.ffiec.gov/

U.S. CERT, OpenSSL “'Heartbleed”' Vulnerability (CVE-2014-0160)
https://www.us-cert.gov/ncas/alerts/TA14-098A)

U.S. CERT, “Heartbleed” OpenSSL Vulnerability
http://www.us-cert.gov/security-publications/Heartbleed-OpenSSL-Vulnerability

Contact:

Donald Saxinger, Senior Examination Specialist, at dsaxinger@fdic.gov or (703) 254-0214

Note:

FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2014/.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- OpenSSL is an open-source implementation of the Secure Sockets Layer and Transport Layer Security protocols. Financial institutions may use OpenSSL in common network services such as Web servers, email servers, virtual private networks, instant messaging, and other applications.
- A significant vulnerability has been found in OpenSSL that could allow an attacker to decrypt, spoof, or perform attacks on network communications that would otherwise be protected by encryption.
- The FDIC expects financial institutions to upgrade vulnerable systems as soon as possible, following appropriate patch management practices.
- Financial institutions should monitor the status of their third-party service providers and vendors’ efforts to implement patches on software that uses OpenSSL and to take the following steps, as appropriate:
    - Ensure that third-party vendors that use OpenSSL on their systems are aware of the vulnerability and take appropriate risk mitigation steps.
    - Monitor the status of their vendors’ efforts.
    - Identify and upgrade vulnerable internal systems and services.
    - Follow appropriate patch management practices[1] and test to ensure a secure configuration.
- Examination guidance and additional information on patch management, software maintenance, and security updates can be found in the following FFIEC IT Examination Booklets:
    - Development and Acquisition
    - Information Security
    - Operations

[1] Patch management, software maintenance, and security update practices are covered by a number of FFIEC IT Examination Handbooks including Development and Acquisition, Information Security, and Operations.