



Financial Cybercrime Task Force of Kentucky

Technical Alert

April 11, 2014

Alert Reference # A0414-01

Subject: Urgent Alert: Cybersecurity vulnerability in OpenSSL (Heartbleed Bug)

The DFI's Financial Cybercrime Task Force of Kentucky (FCTFK) alerts the financial services industry in Kentucky about a critical security vulnerability in OpenSSL that may put systems at risk.

Background: OpenSSL is a cryptographic library commonly used in a wide range of online services to protect the confidentiality of data in transit.

Recommendations: The Department urges state-chartered financial institutions to immediately take the risk mitigation steps outlined in the FFIEC alert issued on April 10, 2014 (<http://www.ffiec.gov/press/PDF/OpenSSLAlert041014.pdf>), produced in part herein as follows:

Server software vendors are working to incorporate a patched version of OpenSSL into their systems. Financial institutions should 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; and*
- *Follow appropriate patch management practices and test to ensure a secure configuration.*

Financial institutions should also consider replacing private keys and X.509 encryption certificates after applying the patch for each service that uses the OpenSSL library. Financial institutions should operate with the assumption that encryption keys used on vulnerable servers are no longer viable for protecting sensitive information and should therefore strongly consider requiring users and administrators to change passwords after applying the OpenSSL patch.

Financial institutions are encouraged to establish mechanisms for obtaining threat and vulnerability information such as through the United States Computer Emergency Readiness Team (US-CERT) portal at www.us-cert.gov or through the Financial Services Information Sharing and Analysis Center (FS-ISAC) at www.fsisac.com.

The following are alerts from other agencies:

- <http://www.ffiec.gov/press/PDF/OpenSSLAlert041014.pdf>
- <http://www.fdic.gov/news/news/financial/2014/fil14016.html>
- http://www.nafcu.org/News/2014_News/April/FFIEC_urges_CUs_banks_to_address_Heartbleed_issue/
- <http://www.us-cert.gov/ncas/alerts/TA14-098A>

If you have any questions regarding this Alert, please contact dfi.reporting@ky.gov.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry and its customers. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, <http://kfi.ky.gov>, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.