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

Financial Institution Letter
FIL-49-2014
September 29, 2014

Technology Alert: GNU Bourne-Again Shell (Bash) 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 with Linux and Unix operating systems that could allow an attacker to gain control of a bank's servers remotely. The vulnerability is commonly known as the GNU Bourne-Again Shell (Bash) or "Shellshock" vulnerability.

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:

Bourne-Again Shell (Bash) "Shellshock" Vulnerability Alert

Related Topics:

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

GNU Bourne-Again Shell (Bash) "Shellshock" Vulnerability (CVE-2014-6271 and CVE-2014-7169)
https://www.us-cert.gov/ncas/alerts/TA14-268A

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:

- Bash is a software tool found on operating systems such as Linux and Unix and is used to translate user instructions and other inputs into machine-readable commands.
- Financial institutions may have Bash present on a wide array of servers and network devices including web servers, email servers, and physical security systems.
- Exploiting this vulnerability may allow attackers to potentially eavesdrop on encrypted communication, steal login credentials or other sensitive data, impersonate financial institution services or users, access sensitive email, or gain access to internal networks.
- Financial institutions should assess whether this software is used within their institutions, and implement patches and upgrades following appropriate patch-management practices. Institutions should also monitor the status of their third-party service providers' and vendors' efforts to implement patches on software where Bash is present.
- 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

Financial institutions should review U.S. CERT, GNU Bourne-Again Shell (Bash) "Shellshock" Vulnerability (CVE-2014-6271 and CVE-2014-7169) for additional information (see https://www.us-cert.gov/ncas/alerts/TA14-268A).