Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

OpenSSL "Heartbleed" Vulnerability Alert

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members[1] are advising financial institutions of a material security vulnerability in the OpenSSL cryptographic library that may put systems that use this encryption method at risk. OpenSSL is an open-source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols commonly used to protect data in transit.

BACKGROUND

OpenSSL is a popular open-source code library for implementing encryption in websites, e-mail servers, and applications and is used in common network services such as web servers, email servers, virtual private networks (VPN), instant messaging, and other applications. Financial institutions may use OpenSSL to cryptographically authenticate their servers to customers, and to protect passwords and other sensitive data from eavesdropping. On April 7, 2014, security researchers reported the existence of a coding error in OpenSSL versions 1.0.1 through 1.0.1f. The vulnerability, nicknamed "Heartbleed," has existed since December 31, 2011.

RISK

The vulnerability could allow an attacker to potentially access a server's private cryptographic keys compromising the security of the server and its users. An attacker may be able to decrypt, spoof, or perform man-in-the-middle attacks on network communications that would otherwise be protected by encryption. Attackers could potentially impersonate bank services or users, steal login credentials, access sensitive email, or gain access to internal networks. Potential attacks are made feasible by the public availability of exploitation tools.

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

RISK MITIGATION

Server software vendors are working to incorporate a patched version[2] 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[3] 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.

REFERENCES

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

FFIEC IT Examination Handbook, Development and Acquisition
http://ithandbook.ffiec.gov/it-booklets/development-and-acquisition.aspx

FFIEC IT Examination Handbook, Information Security
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

FFIEC IT Examination Handbook, Operations

[2] OpenSSL version 1.0.1g
[3] 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.

http://ithandbook.ffiec.gov/it-booklets/operations.aspx