AMERICAN BANKER®
THE FINANCIAL SERVICES DAILY

Friday April 11, 2014

FFIEC Issues Heartbleed Warning; Major Banks Say They're Protected

By Mary Wisniewski and Marian Raab

As regulators told financial institutions Thursday to figure out fixes to a website software coding error that could put some online and mobile banking applications at risk, banks assured customers that their online sites are fine. A few lingering vulnerabilities may remain, however, in banks' networks that will take time to find and patch.

The Federal Financial Institutions Examination Council said Thursday that it expects "financial institutions to incorporate patches on systems and services, applications, and appliances using OpenSSL and upgrade systems as soon as possible to address the vulnerability."

OpenSSL is open-source software that lets web sites encrypt communications with visitors. A 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 bug, nicknamed Heartbleed, has been around since 2012 and was announced by researchers on Monday. It has opened up a window to let attackers steal information such as user names and passwords and the private keys sites use to encrypt and decrypt sensitive data.

"Financial institutions should consider replacing private keys and X.509 encryption certificates after applying the patch for each service that uses OpenSSL and consider requiring users and administrators to change passwords after applying the patch," the FFIEC said. "Financial institutions relying upon third-party service providers should ensure those providers are aware of the vulnerability and are taking appropriate mitigation action."

Many large banks and online banking vendors contacted say their sites and software are not at risk.

Thursday, Bank Technology News ran websites of the largest banks through a Heartbleed bug "checker" run by LastPass, a provider of a password storage service. All were found to be safe except Citigroup's, which was termed "Possibly Unsafe" in that it might use OpenSSL. LastPass recommended that users wait for the site to upgrade before changing their passwords.

Earl Crane
Promontory Financial Group

On Friday, a Citi spokesperson told BTN, "In our standard technology for our customer-facing retail banking and credit card sites and mobile apps we do not use OpenSSL." LastPass updated its site Friday, and a fresh check of Citi's website found it to not be vulnerable.

Bank of America, Capital One Financial, JPMorgan Chase, Citigroup, TD Bank, U.S. Bancorp, Wells Fargo and PNC Financial Services Group have all publicly stated that they are not vulnerable to the Heartbleed bug. Most have said they do not use OpenSSL. A PNC spokesperson told BTN, "We have tested our online and mobile banking systems and confirmed that they are not vulnerable to the Heartbleed bug."

Several online banking vendors have also said they are clear of the security problem.

Scott Hansen, senior vice president of marketing at D+H USA, says that his threat and incident management team "immediately began evaluating the vulnerability with OpenSSL [on April 8], and worked in conjunction with its technology partners in hardware, software, and security to ensure that the necessary measures were in place to prevent compromise to our systems. "As part of our normal process, D+H will continue to monitor the situation in conjunction with the security community and our technology partners."

Wade Arnold, who works under Jack Henry's ProfitStars' division, said in a BTN LinkedIn discussion that the vendor has regenerated all SSL certificates, renewed all open authorization tokens for mobile users and forced the reset of all passwords.

A spokesperson for core banking provider Fiserv said in a statement that the company has been working since the OpenSSL issue was identified to assess and minimize any potential risk to clients. "We have no evidence that any of our systems have been improperly accessed due to this issue," he stated.

Online banking vendor Digital Insight says its websites are not affected because they do not use OpenSSL. The company also says it will continue to investigate, with the help of third-party vendors.

Assuming most banks and vendors have a similar story of non-vulnerability, two problematic scenarios remain for banks with regard to Heartbleed.

One is that they could be indirectly affected by vulnerabilities that existed for some time in the past two years at other sites their customers use, such as Google and Yahoo. These companies have applied patches to their websites, but there's a chance that hackers could have stolen bank customers' passwords from those servers while the sites were vulnerable and could be trying to use those passwords on online banking sites, assuming that consumers use the same passwords for everything, as many do. Security experts urge consumers to change their passwords after the websites they use have run the available patch.

Banks could thwart this type of "replay attack" with the use of stronger authentication, points out Earl Crane, senior principal at Promontory Financial Group. Banks that require a third factor of authentication, such as geolocation, device ID, or a biometric form of identity such as a voice print, could still block hackers who extracted a customer user name and password from a flawed site.

"Under the FFIEC authentication guidance, the reliance on only a user name and password is not sufficient," he observes.

In scenario two, some device in a bank, such as a network router, uses a version of OpenSSL that contains the coding flaw and has not been patched, and that hackers trolling for Heartbleed could find and exploit these vulnerabilities.

Network provider Cisco issued a warning on its website Thursday that several of its products use a vulnerable version of OpenSSL that could allow an unauthenticated, remote attacker to retrieve data from a connected client or server. The list of affected Cisco products is long. The company says it will release free software updates that address these vulnerabilities, and that workarounds that mitigate these vulnerabilities may be available.

Crane points out that such devices are only a risk if they are connected to the internet. "If the vulnerable network equipment is internal-facing, particularly if it's not using the OpenSSL library or OpenSSL is on the device but turned off, it's low risk," he says.

The bigger risk, in his view, is products from vendors that are not releasing patches. "If you have vendors that are out of service agreement, or products that have gone past end of life and are no longer being supported, or if you have a vendor that's slow to issue patches, you're in a more difficult situation," he says. "You either have to wait for your vendor or try to update it yourself." ▪

Penny Crosman contributed to this story.

©2014 SourceMedia Inc. and American Banker. All rights reserved. SourceMedia, One State Street Plaza, New York, N.Y. 10004 (800) 367-3989