Falha grave no OpenSSL pode comprometer dados de usuários de diversos serviços

Foi revelada na segunda-feira (07/04/2014) uma falha grave no protocolo OpenSSL, este protocolo é utilizado por 2 servidores a cada 3. Este protocolo serve para criptografar os dados, como por exemplo, a senha de um usuário.

O OpenSSL utiliza um recurso chamado "heartbeat" (batimento cardíaco), que é usada para manter viva a conexão e alguns protocolos. Justamente neste recurso que foi encontrada uma brecha, que recebeu o apelido de "heartbleed" (sangramento cardíaco). Durante essa brecha podem ser lidos 64 KB de dados aleatórios, porém o processo pode ser repetido diversas vezes, só para se ter uma ideia, em um teste foram necessários apenas 5 minutos para obter 200 nomes e senhas do Yahho! Mail.

A falha já foi resolvida, porém muitos sites ainda não aplicaram a atualização do OpenSSL, o que os especialistas recomendam é que os usuários alterem suas senhas, abaixo alguns sites que foram atingidos e que não foram:

Site/Serviço / E-mail	Trocar Senha?
Facebook	Sim
Instagram	Sim
LinkedIn	Não
Pinterest	Sim
Tumblr	Sim
Twitter	Recomendável
Apple	Recomendável
Amazon	Não
Google	Sim
Microsoft	Não
Yahoo	Sim
AOL	Não
Gmail	Sim
Hotmail / Outlook	Não
Yahoo Mail	Sim
Dropbox	Sim

Pesquisadores da Codenomicon Defensics disponibilizaram um site, http://filippo.io/Heartbleed, onde você pode verificar se um site tem ou já resolveu o problema.

Fonte:

http://www.diario24horas.com.br/noticia/24131-falha-no-openssl-compromete-dados-sigilosos-de-usuarios

http://g1.globo.com/tecnologia/noticia/2014/04/falha-grave-vaza-dados-de-dois-em-cada-tres-sites-seguros-da-web.html

http://info.abril.com.br/noticias/seguranca/2014/04/falha-grave-no-openssl-deixa-dados-sigilosos-vulneraveis-em-servidores-pela-web.shtml

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/