

Social Networks

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Facebook	Unclear	Yes	Yes	"We added protections for Facebook's implementation of OpenSSL before this issue was publicly disclosed. We haven't detected any signs of suspicious account activity, but we encourage people to ... set up a unique password."
IFTTT	Yes	Yes	Yes	IFTTT emailed all its users and logged them out, prompting them to change their password on the site.
Instagram	Yes	Yes	Yes	"Our security teams worked quickly on a fix and we have no evidence of any accounts being harmed. But because this event impacted many services across the web, we recommend you update your password on Instagram and other sites, particularly if you use the same password on multiple sites."
LinkedIn	No	No	No	"We didn't use the offending implementation of OpenSSL in www.linkedin.com or www.slideshare.net . As a result,

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				HeartBleed does not present a risk to these web properties."
Pinterest	Yes	Yes	Yes	"We fixed the issue on Pinterest.com , and didn't find any evidence of mischief. To be extra careful, we e-mailed Pinnerers who may have been impacted, and encouraged them to change their passwords."
Tumblr	Yes	Yes	Yes	"We have no evidence of any breach and, like most networks, our team took immediate action to fix the issue."
Twitter	No	Yes	Unclear	Twitter wrote that OpenSSL "is widely used across the internet and at Twitter. We were able to determine that [our] servers were not affected by this vulnerability. We are continuing to monitor the situation." While reiterating that they were unaffected, Twitter told <i>Mashable</i> that they did apply a patch.

Other Companies

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Apple	No	No	No	"iOS and OS X never incorporated the vulnerable software and key web-based services were not affected."
Amazon	No	No	No	" Amazon.com is not affected."
Google	Yes	Yes	Yes*	<p>"We have assessed the SSL vulnerability and applied patches to key Google services." Search, Gmail, YouTube, Wallet, Play, Apps and App Engine were affected; Google Chrome and Chrome OS were not.</p> <p>*Google said users do not need to change their passwords, but because of the previous vulnerability, better safe than sorry.</p>
Microsoft	No	No	No	Microsoft services were not running OpenSSL, according to LastPass.
Yahoo	Yes	Yes	Yes	<p>"As soon as we became aware of the issue, we began working to fix it... and we are working to implement the fix across the rest of our sites right now."</p> <p>Yahoo Homepage, Yahoo Search,</p>

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				Yahoo Mail, Yahoo Finance, Yahoo Sports, Yahoo Food, Yahoo Tech, Flickr and Tumblr were patched. More patches to come, Yahoo says.

Email

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
AOL	No	No	No	AOL told <i>Mashable</i> it was not running the vulnerable version of the software.
Gmail	Yes	Yes	Yes*	<p>"We have assessed the SSL vulnerability and applied patches to key Google services."</p> <p>*Google said users do not need to change their passwords, but because of the previous vulnerability, better safe than sorry.</p>

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Hotmail / Outlook	No	No	No	Microsoft services were not running OpenSSL, according to LastPass.
Yahoo Mail	Yes	Yes	Yes	"As soon as we became aware of the issue, we began working to fix it... and we are working to implement the fix across the rest of our sites right now."

Stores and Commerce

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Amazon	No	No	No	" Amazon.com is not affected."
Amazon Web Services(for website operators)	Yes	Yes	Yes	Most services were unaffected or Amazon was

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				<p>already able to apply mitigations (see advisory note here).</p> <p>Elastic Load Balancing, Amazon EC2, Amazon Linux AMI, Red Hat Enterprise Linux, Ubuntu, AWS OpsWorks, AWS Elastic Beanstalk and Amazon CloudFront were patched.</p>
eBay	No	No	No	<p>"eBay.com was never vulnerable to this bug because we were never running a vulnerable version of OpenSSL."</p>

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
GoDaddy	Yes	Yes	Yes	"We've been updating GoDaddy services that use the affected OpenSSL version." Full Statement
Nordstrom	No	No	No	"Nordstrom websites do not use OpenSSL encryption."
PayPal	No	No	No	"Your PayPal account details were not exposed in the past and remain secure." Full Statement
Target	No	No	No	"[We] launched a comprehensive review of all

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				external facing aspects of Target.com ... and do not currently believe that any external-facing aspects of our sites are impacted by the OpenSSL vulnerability."
Walmart	No	No	No	"We do not use that technology so we have not been impacted by this particular breach."

Banks and Brokerages

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Bank of America	No	No	No	"A majority of our platforms do NOT use OpenSSL, and the ones that do, we have confirmed no vulnerabilities."
Capital One	No	No	No	"Capital One uses a version of encryption that is not vulnerable to Heartbleed."
Chase	No	No	No	"These sites don't use the encryption software that is vulnerable to the Heartbleed bug."
Citigroup	No	No	No	Citigroup does not use Open SSL in "customer-facing retail banking and credit card sites and mobile apps"
E*Trade	No	No	No	E*Trade is still investigating.
Fidelity	No	No	No	"We have multiple layers of security in place to protect our customer sites and services."

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
PNC	No	No	No	"We have tested our online and mobile banking systems and confirmed that they are not vulnerable to the Heartbleed bug."
Schwab	No	No	No	"Efforts to date have not detected this vulnerability on Schwab.com or any of our online channels."
Scottrade	No	No	No	"Scottrade does not use the affected version of OpenSSL on any of our client-facing platforms."
TD Ameritrade	No	No	No	TD Ameritrade "doesn't use the versions of openssl that were vulnerable."
TD Bank	No	No	No	"We're currently taking precautions and steps to protect customer data from this threat and have no reason to believe any customer data has been compromised in the past."

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
U.S. Bank	No	No	No	"We do not use OpenSSL for customer-facing, Internet banking channels, so U.S. Bank customer data is NOT at risk."
Wells Fargo	No	No	No	No reason provided.

Government and Taxes

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
1040.com	No	No	No	"We're not vulnerable to the Heartbleed bug, as we do not use OpenSSL."
FileYour Taxes.com	No	No	No	"We continuously patch our servers to keep them updated. However, the version we use was not affected by the issue, so no action was taken."

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
H&R Block	Unclear	No	Unclear	"We are reviewing our systems and currently have found no risk to client data from this issue."
Healthcare .gov	No	No	No	" Healthcare.gov consumer accounts are not affected by this vulnerability."
Intuit (TurboTax)	Yes	Yes	Yes	Turbotax "has examined its systems and has secured TurboTax to protect against the "Heartbleed" bug." Full Statement
IRS	Unclear	Unclear	Unclear	"The IRS continues to accept tax returns as normal ... and systems continue operating and are not affected by this bug. We are not aware of any security vulnerabilities related to this situation."
TaxACT	No	No	No	"Customers can update their passwords at any time, although we are not

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				proactively advising them to do so at this time."
USAA	Yes	Yes	Yes	USAA said that it has "already taken measures to help prevent a data breach and implemented a patch earlier this week."

Other

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Box	Yes	Yes	Yes	"We're currently working with our customers to proactively reset passwords and are also reissuing new SSL certificates for added protection."

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
Dropbox	Yes	Yes	Yes	On Twitter : "We've patched all of our user-facing services & will continue to work to make sure your stuff is always safe."
Evernote	No	No	No	"Evernote's service, Evernote apps, and Evernote websites ... all use non-OpenSSL implementations of SSL/TLS to encrypt network communications." Full Statement
LastPass	Yes	Yes	No	"Though LastPass employs OpenSSL, we have multiple layers of encryption to protect our users and never have access to those encryption keys." Users don't need to change their master passwords

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				because they're never sent to the server . But passwords for other sites stored in LastPass might need to be changed.
Minecraft	Yes	Yes	Yes	"We were forced to temporary suspend all of our services. ... The exploit has been fixed. We can not guarantee that your information wasn't compromised." More Information
Netflix	Unclear	Unclear	Unclear	"Like many companies, we took immediate action to assess the vulnerability and address it. We are not aware of any customer impact."
OKCupid	Yes	Yes	Yes	"We, like most of the Internet, were

	Was it affected?	Is there a patch?	Do you need to change your password?	What did they say?
				stunned that such a serious bug has existed for so long and was so widespread."
SoundCloud	Yes	Yes	Yes	SoundCloud emphasized that there were no indications of any foul play and that the company's actions were simply precautionary.
Spark Networks (JDate, Christian Mingle)	No	No	No	Sites do not use OpenSSL.
Wunderlist	Yes	Yes	Yes	"You'll have to simply log back into Wunderlist. We also strongly recommend that you reset your password for Wunderlist." Full Statement

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