What You Need to Know About Heartbleed, the New Security Bug Scaring the Internet

ABBY OHLHEISER

HEARTBLEED.COM

What should you know about Heartbleed, a recently uncovered security bug? The shortest version: You'll have to change all of your passwords, and temporarily avoid any site that is

known to be vulnerable. That sounds a bit alarmist, we know, but now that internet and security experts know a little more about the security vulnerability, it's becoming more and more clear that Heartbleed is nothing to mess with.

Tumblr users recently heard about Heartbleed thanks to a note sent out by the blogging service encouraging all of its users to change their passwords, immediately. So here's the rundown on what you need to know, and what you can do to protect yourself as much as possible from the fall-out.

So what is it?

Heartbleed is a security vulnerability in OpenSSL, a popular, open-source protocol used to encrypt vast portions of the web. It's used to protect your usernames, passwords, and sensitive information set on secure websites. Lifehacker, who published a great, plain-language guide to the flaw earlier today, notes that about 66 percent of the web probably uses OpenSSL to encrypt data. Security company Codenomicon set up an entire website to handle questions about the vulnerability, although their explanation might be too in the weeds for some readers.

At this point, some sites will be running new, fixed versions of OpenSSL and are already secure, while some may have never upgraded to the years-old version of the protocol that contains the vulnerability in the first place. There are a few tools out there you can use to test whether a site is vulnerable to this flaw. And here's an incomplete list of sites that are indicating they are vulnerable, including Yahoo. A sample:

```
Testing okcupid.com...  vulnerable.
Testing pch.com...  vulnerable.
Testing xda-developers.com...  vulnerable.
Testing steamcommunity.com...  vulnerable.
Testing slate.com...  vulnerable.
Testing scoop.it...  vulnerable.
Testing hidemyass.com...  vulnerable.
Testing 123rf.com...  vulnerable.
Testing m-w.com...  vulnerable.
Testing dreamstime.com...  vulnerable.
Testing amung.us...  vulnerable.
Testing duckduckgo.com... not vulnerable.
Testing leo.org...  vulnerable.
Testing eventbrite.com...  vulnerable.
```

Source

How does it work?

The Verge has a very good explanation, so we'll quote them:

The bug allows an attacker to pull 64k at random from a given server's working memory. It's a bit like fishing — attackers don't know what usable data will be in the haul — but since it can be performed over and over again, there's the potential for a lot of sensitive data to be exposed. The server's private encryption keys are a particular target, since they're necessarily kept in working memory and are easily identifiable among the data. That would allow attackers to eavesdrop on traffic to and from the service, and potentially decrypt any past traffic that had been stored in encrypted form.

In other words, someone could simply pull small bits of data from a server, over and over, until gaining the private keys needed to read all of the information that's there. That's potentially disastrous for both the companies and their users, for reasons that should not need any explaining.

What do I do? What do I do?

Do you Yahoo? Do you use your Yahoo password on other sites? That password was possibly compromised by the security bug, and you'll have to change it once the bug is fixed. But because each system administrator has to manually fix the problem, which takes time, there's really nothing you can do until the compromised sites are up and running with an updated version of OpenSSL, and a new security certificate in place — a "reset" of the encryption used to protect current and archived information on the server going forward. Yahoo is working on a fix, but isn't there yet with all of its properties. Each site affected will have to do the same. Until then, stay away from those sites. It could take days, or longer, for vulnerable sites to recover from the bug.

Flair for drama? Take Tor's advice on Heartbleed: "If you need strong anonymity or privacy on the Internet, you might want to stay away from the Internet entirely for the next few days while things settle."

In any case, its worth noting that even the best fixes to Heartbleed won't completely secure all past web traffic from vulnerability. And, because individual servers have to be fixed manually, some sites might not get around to repairing the bug for quite awhile. In other words, take Heartbleed on a site-by-site basis. Very few sites have offered comprehensive information on what to do about Heartbleed to its users. One would hope that advice will be coming soon.

Who would want to exploit Heartbleed?

You know, anyone with basic programming skills who might want some sensitive user data at their finger tips. Or, as many have suggested, there are some government agencies known to have a fondness for collecting user information and web traffic in bulk. If they knew about it before its exposure, Heartbleed could have been a big Christmas present to those efforts.

SEE COMMENTS (12)