**Here's How To Protect Yourself From The Massive Security Flaw That's Taken Over The Internet**



[Kyle Russell](http://www.businessinsider.com/author/kyle-russell)

Apr. 8, 2014, 9:53 PM 309,912 [59](http://www.businessinsider.com/heartbleed-bug-explainer-2014-4#comments)

Read more: <http://www.businessinsider.com/heartbleed-bug-explainer-2014-4#ixzz2yUFbk6wm>

It's been a while since there was a computer security bug we all had to worry about.

Unfortunately, it seems like we may all have been facing one for two years and not even realized it.

Yesterday, security researchers [announced](http://heartbleed.com/) a security flaw in OpenSSL, a popular data encryption standard, that gives hackers who know about it the ability to extract massive amounts of data from the services that we use every day and assume are mostly secure.

This isn't simply a bug in some app that can quickly be updated. The vulnerability is in the machines that power services that transmit secure information, such as Facebook and Gmail.

We've put together the following guide to the so-called Heartbleed bug for those who want to understand what all the fuss is about, and how they can protect themselves.

**What is the Heartbleed bug?**

Heartbleed is a flaw in OpenSSL, the open-source encryption standard used by the majority of websites that need to transmit the data that users want to keep secure. It basically gives you a secure line when you're sending an email or chatting on IM.

Encryption works by making it so that data being sent looks like nonsense to anyone but the intended recipient.

Occasionally, one computer might want to check that there's still a computer at the end of its secure connection, and it will send out what's known as a heartbeat, a small packet of data that asks for a response.

Because of a programming error in the implementation of OpenSSL, the researchers found that it was possible to send a well-disguised packet of data that looked like one of these heartbeats to trick the computer at the other end into sending data stored in its memory.

The flaw was first reported to the team behind OpenSSL by Google security researcher Neel Mehta, and independently found by security firm [Codenomicon](http://www.codenomicon.com/). According to the researchers who discovered the flaw, the code has been in OpenSSL for about two years, and using it doesn't leave a trace.

**How bad is that?**

It's *really*bad. Web servers can keep a lot of information in their active memory, including usernames, passwords, and even the content that users have uploaded to a service. According to [Vox.com's Timothy Lee](http://www.vox.com/2014/4/8/5593654/heartbleed-explainer-big-new-web-security-flaw-compromise-privacy), even credit-card numbers could be pulled out of the data sitting in memory on the servers that power some services.

But worse than that, the flaw has made it possible for hackers to steal encryption keys — the codes used to turn gibberish-encrypted data into readable information.

With encryption keys, hackers can intercept encrypted data moving to and from a site's servers and read it without establishing a secure connection. This means that unless the companies running vulnerable servers change their keys, even future traffic will be susceptible.

**Am I affected?**

Probably, though again, this isn't simply an issue on your personal computer or your phone — it's in the software that powers the services you use. Security firm Codenomicon [reports](http://heartbleed.com/):

You are likely to be affected either directly or indirectly. OpenSSL is the most popular open source cryptographic library and TLS (transport layer security) implementation used to encrypt traffic on the Internet. Your popular social site, your company's site, commercial site, hobby site, sites you install software from or even sites run by your government might be using vulnerable OpenSSL.

According to a recent [Netcraft web server survey](http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html) that looked at nearly 959,000,000 websites, 66% of sites are powered by technology built around SSL, and that doesn't include email services, chat services, and a wide variety of apps available on every platform.

**So what can I do to protect myself?**

Since the vulnerability has been in OpenSSL for about two years and using it leaves no trace, assume that your accounts may be compromised. You should change your online passwords, especially for services where privacy and security are major concerns. However, many sites likely haven't upgraded to software without the bug, so immediately changing them still might not help.

The researchers who discovered the flaw let the developers behind OpenSSL know several days before announcing the vulnerability, so it was fixed before word got out yesterday. Most major service providers should already be updating their sites, so the bug will be less prevalent over coming weeks.

Read more: <http://www.businessinsider.com/heartbleed-bug-explainer-2014-4#ixzz2yUFT2lzl>