

What you need to know about the Heartbleed bug

April 9 2014, by Bree Fowler

Millions of passwords, credit card numbers and other personal information may be at risk as a result of a major breakdown in Internet security revealed earlier this week.

The damage caused by the ["Heartbleed" bug](#) is currently unknown. The [security hole](#) exists on a vast number of the Internet's Web servers and went undetected for more than two years. While it's conceivable that the flaw was never discovered by hackers, it's nearly impossible to tell.

There isn't much that people can do to protect themselves until the affected websites implement a fix.

Here are answers to some common questions about Heartbleed and how you can protect yourself:

Q: What is Heartbleed and why is it a big deal?

A: Heartbleed affects the [encryption technology](#) designed to protect online accounts for email, instant messaging and e-commerce. It was discovered by a team of researchers from the Finnish security firm Codenomicon, along with a Google Inc. researcher who was working separately.

It's unclear whether any information has been stolen as a result of Heartbleed, but security experts are particularly worried about the bug

because it went undetected for more than two years.

Q: How does it work?

A: Heartbleed creates an opening in SSL/TLS, an encryption technology marked by the small, closed padlock and "https:" on Web browsers to show that traffic is secure. The flaw makes it possible to snoop on Internet traffic even if the padlock is closed. Interlopers can also grab the keys for deciphering encrypted data without the website owners knowing the theft occurred.

The problem affects only the variant of SSL/TLS known as OpenSSL, but that happens to be one of the most common on the Internet.

Q: So if the problem has been identified, it's been fixed and I have nothing to worry about. Right?

A: It depends on the website. A fixed version of OpenSSL has been released, but it's up to the individual website administrators to put it into place.

Yahoo Inc., which has more than 800 million users around the world, said Tuesday that most of its popular services—including sports, finance and Tumblr—had been fixed, but work was still being done on other products that it didn't identify.

Q: So what can I do to protect myself?

A: Ultimately, you'll need to change your passwords, but that won't do any good until the sites you use adopt the fix. It's also up to the Internet services affected by the bug to let users know of the potential risks and encourage them to change their passwords.

© 2014 The Associated Press. All rights reserved.

Citation: What you need to know about the Heartbleed bug (2014, April 9) retrieved 20 March 2024 from <https://phys.org/news/2014-04-heartbleed-bug.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.