Protect yourself against the Heartbleed security error

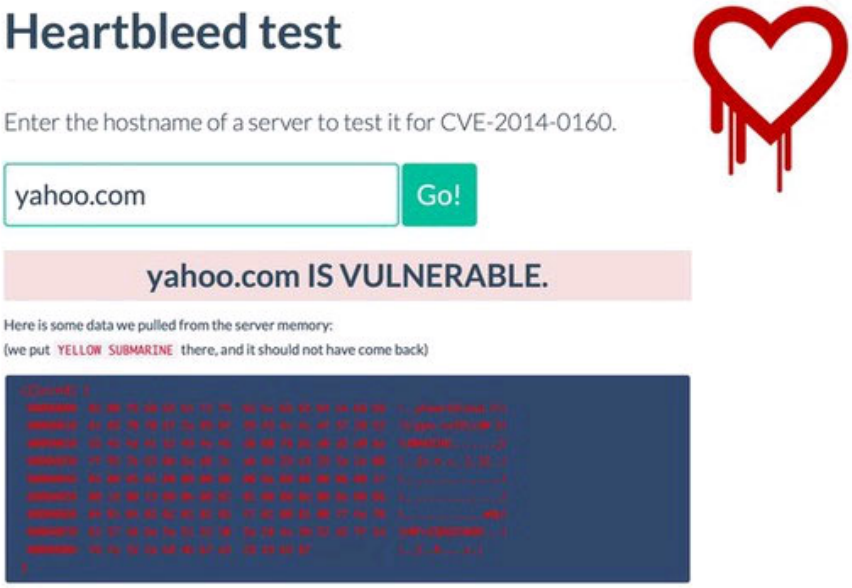
Security experts offer advice to help users protect themselves safe from the security hole Heartbleed is spreading terror to the web world.

Security experts offer advice to help users protect themselves safe from the security hole Heartbleed is spreading terror to the web world.

A new security hole discovered earlier this week called Heartbleed is spreading terror to the internet world. Heartbleed is an **OpenSSL** security standard error used by many websites, and this newly discovered OpenSSL vulnerability can help hackers access the memory of web servers, which store user data. , including sensitive data such as account name, password, and credit card number. This is a serious security error, even rated as the biggest security hole on the web.

According to *Netcraft* researchers , *Heartbleed* affects 500,000 servers worldwide. Therefore, before the security world can find a way to overcome it thoroughly, users need to protect themselves.

Do not log in to affected websites



This is something you need to avoid first. You should not log into affected sites until you are sure that the site has fixed the **Heartbleed** error (*through the website's notifications to you*). If necessary, you should contact their customer service team to update information.

Currently, some websites seem to have been affected by Heartbleed including Yahoo! and the website for *OKCupid* dating service, although these companies said they had overcome " *whole* ", or " *one part"* . You can also check the security of the site **here** , see the list of sites suspected of being stuck with Heartbleed **here** . However, even if this tool says the website is " *safe* ", you should be cautious; In the case of the tool on the red sign, you should avoid the site.

In Vietnam, most online payment sites have Heartbleed errors, since these sites all use *OpenSSL* security technology. Only payment gateway Soha is not affected by the *PCI DSS* security standard - the highest security standard guaranteed by the *Master Card* . According to the research, some error-free payment portal Heartbleed has timely overcome to ensure safety.

With security errors, users often think about changing passwords, but in this case, security experts recommend waiting for the affected webite to fix Heartbleed first, by changing the password at once. not effective even exacerbates the problem.

Change Password

As mentioned above, when the website fails to confirm that they have fixed the security vulnerability, you should immediately change your password and other sensitive personal information. Even if the services you use apply 2-layer security (*transaction confirmation via phone message*), changing your password now is a good thing to do.

Keep track of recent transactions

When the Heartbleed vulnerability allows hackers to access the memory of servers, the risk of your sensitive information, such as credit card numbers, is in their hands. Therefore, you need to keep track of your financial transactions in recent times to see if something is wrong.

Avoid other risks

Even if you have followed the above tips, it does not mean that you are secure. Because according to security experts, Heartbleed even affects cookies - a tool to track user activities when they surf the web. This means that when you access a webite that is affected by Heartbleed, even if you do not log in to the website, you are at risk of stealing information. According to *Tor Project* - a network system for anonymous access and high security - users can, if possible, stay away from the Internet completely for a few days until all vulnerabilities are thoroughly fixed.

Among current web services, Yahoo! seems to be the name with the highest risk of errors (*preliminary tests show that the web version of Facebook, Google, and Twitter, seems to be safe*). Yahoo! They said they have *"taken reasonable remedy"* for their main services including *Yahoo !, Search, Mail, Finance, Sports, Food, Tech, Flickr and Tumblr.* But there are still many other Yahoo! has not been fixed and the company said it is actively fixing bugs for those sites.

Jaime Blasco , director of the *AlienVault Labs* security research *lab* , encourages users not to log into Yahoo! and other affected services, because their sensitive personal information may be stolen. The researcher also advised users to immediately change the password immediately after Yahoo! overcome the above hole.

Not only Yahoo! but other companies like *Imgur* and *OKCupid are* also attacked by Heartbleed. *Imgur* , a very popular photo-sharing website, is now one of them. However, it seems that these companies have quickly come up with corrective measures. Imgur said it has *"reset"* sensitive data such as cookies and session IDs to ensure safety; OKCupid also has a similar statement.

Solution for the future

Cases like Heartbleed are taking place more and more and cause many concerns about the security of web companies today. Currently, some big technology firms are starting to apply **Perfect Forward Secrecy** (*PFS*) security technology but its application is not yet thorough. PFS is a new encryption technology in which the encryption key does not exist forever, making hackers even with encryption keys unable to steal data.

" *Users always want their data to be as secure as possible, and PFS is the tool that web companies need to apply to serve this requirement,* " said *John Miller* , director of *TrustWave* security firm.

You finished reading the article "**Protect yourself against the Heartbleed security error**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.