McAfee
An Intel Company

Consumer Threat Alert

HEARTBLEED

Dear Eric:

Recently, a major security vulnerability named "Heartbleed" has made headlines around the world. This is a severe vulnerability stemming from a coding mistake in a widely-used security utility called OpenSSL.

The bug affects the encryption technology designed to protect your sensitive data on the Internet, like usernames, passwords and emails.

This is a flaw in the OpenSSL encryption code, not a virus that can be stopped by McAfee or other consumer security software. Because this vulnerability takes advantage of servers, and not consumer devices, businesses need to update to the latest version of OpenSSL to mitigate and address the dangers posed.

McAfee is currently in the process of auditing all of our services, and the services provided by our partners, for any dangers posed by Heartbleed. If there is any instance that the vulnerable version of OpenSSL is in use we will remediate with the utmost urgency.

The severity of the Heartbleed vulnerability cannot be overstated: several major enterprises use OpenSSL, and are likely affected by this vulnerability as well. The dangers posed by this vulnerability are very real and could affect you if exploited.

So what do you need to do?

- Right now, the best thing you can do is wait to be notified about affected services and patches or you can investigate this list provided by Mashable that has some well known brands listed.
- If you'd like to investigate whether or not a website you frequent has been affected, you can use this tool.
- Reset your password for every online service affected by Heartbleed. But beware: **you should only change your password after the afflicted business has fixed its servers to remove the Heartbleed vulnerability.** Changing your passwords before a company's servers are updated will not protect your credentials from being leaked.
- For additional details, please click here.

We at McAfee apologize for any inconvenience this may cause you. We will be contacting you again as we update our services that use OpenSSL.

Thank you for your time, and safe surfing.

Sincerely,

Gary Davis