Assurant Websites and Applications Safe from Heartbleed Bug

Assurant's websites and applications are not compromised by the "Heartbleed" bug, a security flaw that could make it easier for hackers to access personal information submitted by users visiting a website.

Assurant Corporate Technology (ACT) Information Security and Technology teams began to scan the company's network to determine vulnerabilities upon the disclosure of the security flaw in OpenSSL, the open source encryption standard many websites on the internet use that encrypts and protects communication between a computer and a website. Assurant uses encryption technology on its websites to protect both client and consumer information as it is submitted online.

The "Heartbleed" bug is a security flaw in encryption technology that makes websites vulnerable to data theft by hackers. Assurant's websites and applications are not compromised by this threat.

 "We determined that our web servers, firewalls, email gateways and internet traffic load balancers are not susceptible to the Heartbleed bug," said Marilyn Piccolo, vice president, Information Security Office of Assurant, Inc. "As a precaution, however, we advise customers to change their passwords in light of the threat especially if you use the same user name and password across various accounts."

The company also is working with its business partners to ensure encrypted communications from Assurant to them were not compromised. If a business partner was compromised by the security flaw, Assurant will issue new encryption keys after the OpenSSL vulnerability is remediated to ensure secure communication.

"Securing our customers' information is a high priority for us and we take this matter very seriously," said Piccolo. "We will continue to monitor our systems for any other potential threats and adapt new security strategies and protocols as needed."

Cyber risks like the Heartbleed bug can expose consumers to unintentional or unauthorized sharing of information. Assurant has adopted strict data security measures to protect client and consumer information. If you are a business partner and have concerns about the Heartbleed bug, please contact Assurant through your normal support channels.