NovaVision

NovaVision Inc.'s Statement on the Heartbleed OpenSSL Vulnerability
2014-04-16

Recently, the Heartbleed bug was reported in some versions of OpenSSL, which is used to encrypt data sent over the Internet. The Heartbleed bug allows fraudsters to eavesdrop on communications, to steal data directly from the services and users and to impersonate services and users.

We are happy to report that our Internet servers did not use the affected versions of OpenSSL. Therefore our Internet applications were not, and had never been, vulnerable to Heartbleed including all our web sites and shopping carts at these URL's:

www.novavisioninc.com
www.tamper.com
www.thermalimages.com

Because information you entered at any one of our web sites was NOT at risk due to the Heartbleed vulnerability, you do not need to change any UNIQUE passwords you use for our web sites.

However, if you use an email address and password combination on our site that you also use on another site that was or is vulnerable to Heartbleed, we recommend you log into all accounts(s) -- our site included -- and change your passwords.

If a site has a vulnerability, and has not yet patched OpenSSL, then changing your password is not helpful at this time.

You can check whether web sites are vulnerable (including ours) at the Heartbleed test: https://filippo.io/Heartbleed/

For more information on Heartbleed: http://heartbleed.com/

Andrew Leitner
IT Manager
NovaVision Inc.

524 East Woodland Circle, Bowling Green, OH 43402
Phone: 419-354-1427 Fax: 419-353-7908 www.novavisioninc.com