STRATEGIC INFORMATION TECHNOLOGY LTD.

SIT
Corporate Communications

April 10, 2014

Portfolio Plus is not Directly Affected by OpenSSL Vulnerability. SIT Encourages All Customers To Check Third-Party Products and Service Providers.

Earlier this week a flaw was discovered in OpenSSL, an Internet encryption protocol that is used to secure sessions between consumer devices and websites. SIT does not embed OpenSSL in any Portfolio Plus products.

The "Heartbleed" vulnerability was discovered in the TLS Heartbeat Extension, a portion of OpenSSL protocol that facilitates the exchange of data, and could potentially expose the memory of a vulnerable web server.

SIT is currently assessing all potential vulnerabilities and is responding to clients on a priority basis, as required.

SIT encourages clients to review their own IT infrastructures for any third-party applications that may use OpenSSL.

Clients who have a secure HTTPS website that uses an Apache web server with OpenSSL should check what version of OpenSSL they are using. Anyone using OpenSSL versions 1.0.1 through 1.0.1f and 1.0.2 beta will need to install the latest version, OpenSSL 1.0.1g.

We would also like to encourage our clients to change their passwords regularly.

For more information on the Heartbleed bug, please see www.heartbleed.com.

Sincerely,

Patrick Lannigan
VP Marketing