589 8th Avenue, 8th Floor, New York, NY 10018 | exigis.com

FOR IMMEDIATE RELEASE

Contact: Media
Tel: +1.800.928.1963
Email: media @exigis.com

EXIGIS Confirms No Vulnerability to Heartbleed Bug

EXIGIS confirmed today that its web applications and services are secure and are not susceptible to the Heartbleed vulnerability in OpenSSL.

New York, NY, April 25, 2014 - EXIGIS, LLC., the leading provider of enterprise software and services for risk management, insurance, and trade finance, confirmed today that its systems and RiskWorks' web applications and services are not and have not been susceptible to the recent Heartbleed vulnerability which has impacted numerous servers and websites.

The Heartbleed Bug is a serious software security flaw in OpenSSL, one of the most common security protocols. It allows attackers to eavesdrop on communications and steal data directly from the services, and permits malicious users to impersonate services and user identities. According to OpenSSL, affected versions are 1.0.1 and 1.0.2-beta of OpenSSL (the cryptographic software library) which compromised the security of private information across the internet.

"EXIGIS takes the responsibility of protecting the privacy and security of our customers and partners very seriously," said Kenio Shirley, Manager, Information Technology at EXIGIS. "Within 24 hours of being notified of the potential threat, the EXIGIS Information Service Department conducted a thorough investigation of RiskWorks' servers and services and determined that our products are secure and not affected by the vulnerability."

General information on Heartbleed Bug:

- The Heartbleed Bug exposes computer systems' OpenSSL cryptographic software libraries rendering some SSL/TLS encryption ineffective.
- Applications and passwords affected are web browsers, e-mail, instant messaging (IM) and virtual private networks (VPNs).
- The Heartbleed Bug exposes via Internet, the memory of the systems protected by the vulnerable versions of the OpenSSL software.
- Secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content are exposed.

EXIGIS customers, prospective customers, and partners are encouraged to contact EXIGIS if they have questions or need any additional information regarding Heartbleed by calling (800) 928-1963.

About Heartbleed

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs). The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

More information on this vulnerability visit www.heartbleed.com.

About EXIGIS

EXIGIS is the leading provider of enterprise process automation software and services for risk management, insurance, and trade finance. Since 2002, we have successfully partnered with over 75 leading Fortune class companies, public sector entities, and global insurance brokers to deliver value-driven solutions that mitigate risk and streamline the execution of the most costly, decentralized and paper-intensive business processes.

Exposure Data Management l Insurance Compliance l Certificates of Insurance l Risk Control

For more information on EXIGIS, call (1 800) 928-1963 or email media@exigis.com.

Learn what EXIGIS can do for your business at exigis.com