Contact:
George Faucher
(239) 267-7356
info@correlog.com
www.correlog.com

Media Bulletin

FINAL: FOR DISTRIBUTION

CorreLog, Inc. Issues Statement on Heartbleed Bug

CorreLog Server uses OpenSSL version 0.9.8r 8 Feb 2011, which is not vulnerable to Heartbleed Bug CVE-2014-0160.

Naples, FL, April 21, 2014 – CorreLog, the leader in multi-platform IT security event log management, today issued a formal statement on the Heartbleed Bug, named CVE-2014-0160 by MITRE, a non-profit organization that operates research and development centers sponsored by the federal government. CorreLog's position on Heartbleed Bug CVE-2014-0160 is as follows.

For the three products CorreLog Server, CorreLog Agent for IBM z/OS, and CorreLog SyslogDefender™:

- CorreLog Server uses OpenSSL version 0.9.8r 8 Feb 2011, which does not have this particular Heartbleed vulnerability.
- There are no issues associated with using Apache TLS encryption option obtained by download from the CorreLog, Inc. website, or from any CorreLog Server installation using OpenSSL version 0.9.8r 8 Feb 2011.
- CorreLog, Inc. maintains a strict policy of using only stable and trusted Apache servers and we have found version 0.9.8r 8 Feb 2011 to be highly stable and secure.
- Apache version 0.9.8r 8 Feb 2011 as installed with CorreLog Server requires no upgrade to address the Heartbleed Bug.
    - This is true of all versions of the CorreLog Server Enhanced Encryption Code, including any future versions.
- The CorreLog Agent for IBM z/OS does not use the OpenSSL library for its SSL/TLS support, and thus is not vulnerable to the Heartbleed bug.
- CorreLog SyslogDefender™ provides TLS encryption for Syslogs and does not operate as a web server in the sense that CorreLog Server does, and is therefore an unlikely target for the Heartbleed bug.
    - CorreLog recommends customers using SyslogDefender™ upgrade to the latest build of SyslogDefender™, version 5.4.2 which leverages OpenSSL 1.0.1g (1.0.1g details here).

Contact:
George Faucher
(239) 267-7356
info@correlog.com
www.correlog.com

- SyslogDefender™ version 5.4.2 is available only by contacting CorreLog support (support@correlog.com, or +1-239-514-3331, ext. 2).

More general information on Heartbleed Bug CVE-2014-0160:

- 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.
  - The result allows attackers to eavesdrop on communications and steal data directly from the services, and permits malicious users to impersonate services and user identities.
- More information on this vulnerability can be found at http://heartbleed.com.

CorreLog, Inc. customers, prospective customers, and partners may contact CorreLog support for additional information on Heartbleed, as it pertains to CorreLog Server, the Agent for IBM z/OS and SyslogDefender™.

- E-mail: support@correlog.com
- Toll-free phone (USA): +1-877-267-7356
- Direct/International phone: +1-239-514-3331
- Web: http://correlog.com/support.html.

About CorreLog, Inc.:

CorreLog, Inc. is the leading independent software vendor (ISV) for IT security log management and event correlation. CorreLog's flagship product, the CorreLog Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network modeling, proprietary semantic correlation,

automated help-desk ticketing and reporting functions into a unique multi-platform security solution. CorreLog Server operates across Windows, UNIX, Linux and mainframe platforms, shipping with an out-of-box PCI DSS compliant CorreLog Agent for IBM z/OS, the world's most popular mainframe operating system.

CorreLog Server delivers an essential viewpoint via dashboard console, providing verifiable and actionable information on the activity of users, devices, and applications to proactively meet organizational SLAs and regulatory requirements. Additionally, CorreLog Server automatically identifies and responds to any suspicious behavior, network attacks, or policy violations by indexing and correlating user activity and event logs, then archives the data in a datacenter server location. This allows customer organizations to quickly identify then proactively respond to compliance violations, policy breaches, cyber-attacks and insider threats. For auditing and forensics, CorreLog Server facilitates regulatory requirements set forth by PCI DSS, HIPAA, SOX, FISMA, NERC, NCUA, IRS Pub. 1075 and many other standards. CorreLog, Inc. markets its solutions through both direct and indirect partner channels.

http://www.correlog.com/

###

Copyright © 2014, CorreLog, Inc. All rights reserved.
All trademarks and registered trademarks used herein are the properties of their respective owners.

++++

Press Contact:

George Faucher
George.faucher@correlog.com
www.correlog.com
Toll-free USA: (877) CorreLog
International: +1 (239) 514-3331, ext. 401