Array Networks Unaffected by OpenSSL Heartbleed Vulnerability

Company's products use a proprietary SSL stack to process SSL, TLS and DTLS service traffic and are NOT exposed to the OpenSSL heartbleed vulnerability

MILPITAS, CA–April10, 2014– Array Networks Inc., a global leader in application delivery networking, today announced that Array Networks products are NOT exposed to the OpenSSL Heartbleed vulnerability. Unlike hardware and software vendors who have integrated OpenSSL into their core product and service offerings, Array is unaffected because the company uses a proprietary SSL stack to process SSL, TLS and DTLS service traffic.

As described on the Common Vulnerabilities and Exposures Website, the TLS and DTLS implementations in OpenSSL 1.0.1, before 1.0.1g, do not properly handle Heartbeat Extension packets which allow remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Array products – including APV, vAPV, AG, vxAG and EOS products (TMX, SPX) – usethe company's proprietary SSL stack to process all SSL, TLS and DTLS service traffic. Therefore, service traffic on Array products is not affected by this OpenSSL Heartbleed vulnerability.

In addition, Array products only have limited usage of OpenSSL for WebUI and SSH management. The versions of OpenSSL used by Array products are not affected by the OpenSSL Heartbleed vulnerability so management traffic on Array products is not affected by the vulnerability either.

Not only is Array's proprietary SSL implementation less vulnerable to exposure, it also delivers additional significant advantages to customers. For businesses requiring 2048-bit or 4096-bit SSL acceleration, Array supports industry-leading scalability and performance on every entry-level, mid-range and high-end appliance. Moreover, every Array appliance delivers the lowest cost $/SSL TPS on the market, bar none, and provides an unmatched set of high-performance SSL and certificate handling features.

"As a leader in SSL acceleration and SSL VPN, we are happy to report that Array is not affected by this recent OpenSSL vulnerability," said Michael Zhao, president and CEO of Array Networks. "The time and attention we pay to creating our own implementations not only deliver superior performance, scalability and economics for customers that transact business on the Web, it also ensures that customers are not exposed to vulnerabilities that so often arise from use of open technologies."

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore™ software, Array solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 300 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought

leaders including Deloitte, Red Herring and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Press Contact:
Robert Adler
Vantage PRfor Array Networks
+1 415 984 1970 ext. 0104
radler@vantagepr.com