**FOR IMMEDIATE RELEASE**

# Array Networks Unaffected by OpenSSL DROWN Vulnerability

*Company's load balancing and SSL VPN appliances prove historically less vulnerable as compared to alternative application delivery solutions*

**Milpitas, CA – March 22, 2016** – Array Networks Inc., a global leader in application delivery networking, announces today Array Networks products are NOT exposed to the DROWN vulnerability. Unlike hardware and software vendors that have integrated OpenSSL into their core product and service offerings or rely on SSLv2, Array is unaffected because the company uses a proprietary SSL stack to process SSL, TLS and DTLS service traffic. Array also does not permit the use of the weak SSLv2 protocol.

As described on the DROWN Attack Website, DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data. Measurements indicate 33% of all HTTPS servers are vulnerable to the attack.

Array products – including APV, vAPV, AG, vxAG and even end-of-sale TMX and SPX products – use a proprietary SSL stack to process all SSL, TLS and DTLS service traffic. Therefore, service traffic on Array products is unaffected by the OpenSSL DROWN vulnerability. Further, because the use of SSLv2 is not allowed, the impact of the latest OpenSSL vulnerability is fully mitigated.

Customers using Array application delivery solutions do not need to take any measures to patch or remediate the company's products. Moreover, companies offloading SSL on Array appliances benefit from a "first line of defense" that mitigates exposure to the DROWN vulnerability in the event that other elements in the network are affected.

In addition to being unaffected by the DROWN vulnerability, Array Networks products are also unaffected by other recent vulnerabilities including Heartbleed, BASH and a number of other OpenSSL and general security advisories. Benefitting from a security hardened OS, proprietary SSL stack and additional security-oriented design principles, Array load balancing and SSL VPN solutions continue to prove significantly less vulnerable as compared to alternative application delivery solutions.

"As a leader in application delivery, we are happy to report that Array is not affected by the DROWN 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 250 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. To learn more, visit: www.arraynetworks.com

**Press Contact:**
Lynda Starr
Vantage PR for Array Networks
+1 973 386 5949
lstarr@vantagepr.com