ION Networks
120 Corporate Boulevard, South Plainfield, NJ 07080
Tel: +1 908/546/3900 Fax: +1 908/546/3901
www.apitech.com/ION

Revised April 16, 2014

How to Protect Your ION Networks Products From the 'Heartbleed' OpenSSL Vulnerability

On April 9, 2014, the global technology community was notified of the 'Heartbleed' vulnerability within OpenSSL, the open-source encryption technology that is used to encrypt many network communications, including secure web communication.

ION Networks products *not vulnerable* to the Heartbleed flaw:

Product Family	Version
SM110	All
SA500	All
SA600	All
SA5600	All prior to 1.3.1
SA5600-SAL	All except bundle 1.4.1
PR-RD-DT (aka the RD)	All
PRIISMS	Prior to 2.8.1
ST520	All
ST530	All
Netgard MFD	All

ION Networks products affected by the Heartbleed vulnerability:

Product Family	Version	Resolution
SA5600-SAL	Bundle 1.4.1	Released only to beta customers, Install ION.SEC.3.TGZ
SA5600-IA2	All	Install APP-1.3.1-B27.BIN
PR-RD-DT-IA2 (aka the RD)	All	Install ROUTER-1.3.1-B22.BIN
PRIISMS (IA2)	2.8.1	Install from PRIISMS2.8.x-Heartbleed.zip

ION Networks
120 Corporate Boulevard, South Plainfield, NJ 07080
Tel: +1 908/546/3900 Fax: +1 908/546/3901
www.apitech.com/ION

The vulnerability affected the ION products in the use of the open source tool OpenVPN. OpenVPN creates the tunnels between PRIISMS, RD, and Appliances. If your product is listed as vulnerable above, the product should be patched promptly. After the patch is applied, ION Networks recommends the replacement of the certificates used on each of the appliances and each instance of PRIISMS. Instructions on how to update certificates will be provided with the software patch.

If you have any further questions or concerns, please contact ION Networks Technical Support at +1 908-546-3900 Option 2 or by emailing ion.networks.support@apitech.com.

Thank you,

Peter Paulson
Director of Engineering and Operations