ION Networks
1 Corporate Place South, Piscataway, NJ 08854
Tel: +1 908-546-3900
www.apitech.com/ION

December 14, 2021, update 1

Log4J Vulnerability Statement for Your ION Networks Products

The vulnerability tracked as CVE-2021-44228, is a vulnerability of a package known as log4j. ION Networks products are not Java™ based, and almost all do not use do not use log4j. The products which do not use log4j are not vulnerable to the exploits of CVE-2021-44228.

ION Networks products *not vulnerable* to the Log4J vulnerability:

Product Family	**Version**
Netgard Priledged gateway (NPG)	All
Netgard MFD	All
PR-RD-DT (aka the RD)	All
PRIISMS	All
SA500	All
SA5600	All
SA5600-DEF	All
SA5600-IA2	All
ST520	All
ST530	All

*End of Life

Product Family	**Version**
ASG Guard*	All
ASG Guard II*	All
ASG Guard Plus*	All
ION Secure 3500*	All
ION Secure 5500*	All
SM110*	All
Defender*	All

ION Networks SAL products Log4J vulnerability:

Product Family	**Version**	**Installed ADS Version**	**Notes**
SA5600-SAL	All	All	Potentially Vulnerable, Contact ION Support
SA5600-SAL3	All	Prior to 3.2	Potentially Vulnerable, Upgrade to agent version 2.1.4-B10 and ADS version 3.2
SA5600-SAL3	All	3.2 or 3.3	Not Vulnerable

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