



ICT STATEMENT ON LOG4J VULNERABILITY

VANCOUVER, BC, December 17, 2021 – On December 9, 2021, a zero-day, remote code execute vulnerability used in the open-source, Java-based logging library Apache Log4j was discovered, which hackers can potentially exploit to gain access to company servers, networks, and connected devices.

ICT's intelligent, TCP/IP-enabled products allow users to remotely monitor and control DC power conditions using built-in web-based servers or Simple Network Management Protocol (SNMP).

ICT products DO NOT use the affected library and are not impacted by this vulnerability.

ABOUT ICT

Founded in 1986, ICT provides DC power conversion products for the land mobile radio, fixed wireless broadband, small cell and industrial DC power markets. ICT's DC power supplies, fault-tolerant power systems, voltage converters, battery chargers, power inverters, DC backup systems, and Ethernet-enabled intelligent power supplies and DC power distribution panels are used in emergency response dispatch centers, on board vehicles, and in tower, communications and industrial power sites around the world.

ICT's focus is in using innovation to develop DC power products and solutions that help customers solve their power challenges, while providing the best value and lowest cost of ownership. ICT designs and manufactures all its products from its North American facility.