August 1, 2014

Kanguru Statement Responding to Recent "BadUSB" Coverage

Kanguru recently became aware of reports of a new class of malicious attack called BadUSB which focuses on USB technology. The theory of this attack is that the USB device firmware (the software code which runs computer chips) can be hijacked and overwritten in order to provide some type of host computer access to cyber criminals.

Kanguru's Defender™ series of encrypted USB devices are designed in compliance with NIST's requirement of digitally signing device firmware. Changing the customized, onboard device firmware with an unauthorized, malicious version is not possible. Furthermore, there are self-tests run at startup of the cryptographic module within the USB drive which ensure the integrity of the original firmware. If the self-test fails, the device will not operate. This has been validated by NIST for a range of Kanguru's Defender devices that have achieved FIPS 140-2 Level 3 and Level 2. In addition, Kanguru's Defender devices that have not gone through the FIPS process still have this firmware security feature implemented and are not at risk. Please reference the following link for more information: http://csrc.nist.gov/groups/STM/cmvp/standards.html

Kanguru will monitor this important issue closely as additional details are made known. We will continue to keep our Customers aware of any new developments.

Sincerely,

Nate Cote
Executive Vice President – Product Management
Kanguru Solutions