To: Our Valued Customers, Sales Representatives and Distributors
Date: May 5, 2020
Subject: ON Semiconductor RSL10 and the “SweynTooth” Bluetooth® Low Energy Cybersecurity Vulnerabilities

Recently the FDA and the US Department of Homeland Security issued an alert regarding a public report of multiple Bluetooth Low Energy (BLE) vulnerabilities, referred to as the SweynTooth family of cybersecurity vulnerabilities. The report identifies several publically disclosed BLE vulnerabilities that expose flaws in specific BLE SoC implementations that allow an attacker within radio range to trigger deadlocks, crashes, buffer overflows or the complete bypass of security; and can affect devices using affected BLE software development kits (SDK).

These publically disclosed vulnerabilities were reported to affect devices that incorporate BLE wireless communication technology from a number of vendors. The ON Semiconductor RSL10 Bluetooth Radio (RSL10) is not included on this list.

As a trusted and ethical supplier of semiconductor solutions, we have made it our responsibility to conduct our own internal investigations into the named vulnerabilities and communicate directly with our customers. We can confirm that to date the RSL10 is affected by only three of the vulnerabilities:

- Zero LTK Installation
- Channel Map Deadlock
- DHCheck Skip

The RSL10 SDK 3.3 with the SweynTooth vulnerability fixes was released to www.onsemi.com/rsl10 on April 23, 2020.

While our recommendation is that customers upgrade to SDK 3.3, we realize that some of our customers may not wish to do so. In those cases, the expected behavior related to these vulnerabilities is summarized below.

Vulnerability	Expected Behavior
Zero LTK Installation	Dependent on customer application
Channel Map Deadlock	When a zero channel map is received BLE/HW stops working while the rest of the system, continues their normal functionality. To recover one of the following can apply: - SW can reset BLE HW or an RSL10 reset should be applied, e.g by watchdog reset - While BLE/HW is in deadlock situation, if RSL10 enters sleep power mode without maintaining VDDC, BLE/HW will come back to its normal functionality after wakeup and deadlock will no longer exist. After wakeup, if BLE stack SW uses the zero channel map parameter for BLE link, it can put BLE HW in deadlock again. During connection establishment or in the middle of a BLE link, the BLE link will be disconnected and if after the link loss it goes to sleep and wakes up, no deadlock will be available and system will not need a reset to recover from deadlock.
DHCheck Skip	Dependent on customer application

ON Semiconductor continues to monitor the situation and commits to investigating any further developments. In the meantime, if you have any additional questions or concerns, we invite you to contact your account manager.

Regards,

Michel De Mey
Vice President and General Manager
Signal Processing, Wireless, and Medical Division