ON Semiconductor Customer Communication Regarding RSL10 and the "SweynTooth" Bluetooth® Low Energy Cybersecurity Vulnerabilities

Dear Valued Customer,

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. Specifically, 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 SDKs.

These publically disclosed vulnerabilities were reported to affect devices that incorporate BLE wireless communication technology from a number of vendors, of which, the RSL10 Bluetooth radio from ON Semiconductor was not included.

As a trusted and ethical supplier of semiconductor solutions, we have made it our responsibility to conduct our own internal investigations into the vulnerabilities and to communicate directly with our customers. We can confirm that to date the RSL10 is affected by only 1 of the vulnerabilities, the Security Bypass for Zero LTK Installation (CVE-2019-19194).

We are actively working with our BLE stack vendor who is prioritizing their development efforts to provide us with a maintenance release to counter the potential threat of the Security Bypass for Zero LTK installation vulnerability. Once received, we will be conducting extensive testing and verification with plans to incorporate a patch into an SDK release no later than the end of April, 2020.

ON Semiconductor is treating this matter seriously. We continue to monitor the situation and commit to investigating any further developments.

In the meantime, if you have any additional questions or concerns, we invite you to contact your account manager.