

SweynTooth Bluetooth Vulnerabilities

Publication Date: 2020-03-13

Last Update: 2019-03-12

Description

on February 2020, a set of 12 vulnerabilities, named “SweynTooth,” associated with a wireless communication technology known as Bluetooth Low Energy (BLE). BLE allows two devices to “pair” and exchange information to perform their intended functions while preserving battery life.

Product Status

After thorough analysis, SuperSonic Imagine’s Teams have concluded that no products are impacted by the SweynTooth vulnerabilities.

Additional Information:

For additional information on these vulnerabilities, please visit:

- ICS Alert ([ICS-ALERT-20-063-01](#))
- FDA Safety Communication on [SweynTooth](#)
- FDA news Release: [FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy](#)
- Singapore university of Technology and Design [vulnerability Disclosure](#)

For further information on product’s security please visit our product security page:
<https://www.supersonicimagine.com/security>

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.