

Vantive Product Security Bulletin

RE: SweynTooth Vulnerabilities

Publication Date: March 9, 2020

Update Date: March 9, 2020

SUMMARY

Vantive is currently monitoring the Bluetooth Low Energy (BLE) vulnerabilities that were disclosed by researchers from the Singapore University of Technology and Design. The researchers have disclosed 12 vulnerabilities with the potential for more to be identified and released. These vulnerabilities are reported to affect several different BLE system-on-chip (SoC) manufacturers utilizing various affected software development kits (SDK). The vulnerabilities expose flaws in specific BLE SoC implementations that allow an attacker in radio range to trigger deadlocks, crashes, buffer overflows, or the complete bypass of security. The Department of Homeland Security Cybersecurity Infrastructure Security Advisory published ICS Alert ICS-ALERT-20-063-011¹ on March 3, 2020, for this set of vulnerabilities.

RESPONSE

An initial assessment has been completed and it has been determined that no Vantive products use an impacted version of Bluetooth. Vantive will continue to monitor all available information and we will provide an update to this bulletin if necessary.

¹<https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01>