CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Security Advisory related to BlueBorne Attack Vectors in ecom mobile Devices

Document ID TDOCT-6392_ENG
Publication date 2019-03-14

Vulnerabilities or CVE Identifier

CVE-2017-0781, CVE-2017-0785, CVE-2017-0782, CVE-2017-0783 and CVE-2017-8628

Severity

8.8 (CVSS:3.0/ AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products

i.roc Ci70-Ex, Cx70-Ex, CT50-Ex, Pad-Ex 01, Tab-Ex 01,
Smart-Ex 01, Smart-Ex 201, Ex-Handy 09, Ex-Handy 209

Vulnerability Type

Information Leak / Disclosure (CWE-200)
Improper Access Control (CWE-284)

Summary

A collection of Bluetooth attack vectors were discovered and related vulnerabilities known as "BlueBorne" were disclosed. These vulnerabilities collectively endanger amongst others Windows, Linux and mobile operating systems like Android or IOS. An unauthenticated attacker may take control of devices and perform commands or access sensitive data.

Impact

An unauthenticated, remote attacker may be able to obtain private information about the device or user, execute arbitrary code on the device or perform a virtually invisible Man-in-the-middle (MitM) attack.

Solution

Customers using affected Pepperl+Fuchs / ecom instruments products are recommended to update the device. For released firmware updates see table below.

Product	Date	Updatesource
CT50-Ex Android	09/2017	FOTA-Update
CT50-Ex Windows	10/2017	Microsoft Update
Pad-Ex 01	09/2017	Microsoft Update
Smart-Ex 01	09/2018	FOTA-Update
Smart-Ex 201	10/2018	FOTA-Update

In case for a device is no update available, users should consider the following workaround:
Deactivation of Bluetooth on the device

Unused or not needed Bluetooth should be switched off / disabled on affected devices.

Reported by

These vulnerabilities were publicly disclosed by Ben Seri and Gregory Vishnepolsky of Armis.

https://www.armis.com/blueborne/

Support

For support please contact your local Pepperl+Fuchs sales representative.