

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Android Privilege Elevation Vulnerability in ecom mobile devices

Document ID TDOCT-6241_ENG
Publication date 2018-10-20

Vulnerabilities or CVE Identifier

CVE-2018-14825

Severity

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

Affected products

CT50-Ex

Vulnerability Type

Improper Privilege Management (CWE-269)

Summary

An attacker may gain access (by elevated privileges) to CT50-Ex mobile computers through a vulnerability in a system service running the Android Operating System (OS). The system service improperly validates incoming connection requests. Although the vulnerability is significant, currently no known exploits publicly available.

Impact

A skilled attacker with advanced knowledge of the target system could exploit this vulnerability by creating an application that would successfully bind to the service and gain elevated system privileges. This may enable the attacker to obtain access to keystrokes, passwords, personal identifiable information, photos, emails, or business-critical documents.

Solution

An update is available that resolves this vulnerability. All customers using the impacted products should update their products as indicated in the chart below. Only products listed below are affected by this vulnerability. Updates are available via the Pepperl+Fuchs / ecom product support channel or directly from the original manufacturer Honeywell at <https://hsmftp.honeywell.com>.

Pepperl+Fuchs strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Product	Software	Status
CT50-Ex	Android 6.0	Update to CommonES 4.01.00.4134 or later Update ECP to version 2.30.00.0167 or later (if applicable)
	Android 4.4	Update to CommonES 3.17.3445 or later

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