Product Security Notice:
Honeywell Mobile Computers - Android Privilege Elevation Vulnerability

Publish Date: 09-13-2018

CVSS v3.0 Base Score: 7.6

Reference: ICS-CERT Advisory: ICSA-18-256-01

CVE: CVE-2018-14825

Summary

A vulnerability in a system service on CT60, CN80, CT40, CK75, CN75, CT50, D75e, CN51 and EDA series mobile computers running the Android Operating System (OS) could allow a malicious third-party application to gain elevated privileges. The vulnerability exists because the software improperly validates incoming connection requests.

While the vulnerability is significant, no known exploits have been found.

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.

Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Recommended Action

Honeywell has released software updates that resolve 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 at https://hsmftp.honeywell.com or from Honeywell through your product support channel.

Product Name	Software	Status
CT60 CN80 CT40	Android 7.1	(GMS version) Upgrade to Android OS release **84.00.11** or later (non-GMS version) Upgrade to Android OS release 83.00.11 or later
CK75 CN75 CN75e	Android 6.0	Update CommonES to 4.02.00.4082 or later Update ECP to version 2.30.00.0167 or later (if applicable)
CT50 D75e	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
CN51	Android 6.0	Update to CommonES 4.01.03.3992 or later Update ECP to version 2.30.00.0167 or later (if applicable)
EDA50k	Android 4.4	Update to CommonES 3.17.3321.10 or later Release will be available: 9/21/2018
EDA50 EDA50k EDA70	Android 7.1	Update to CommonES 5.01.01.4217 or later Release will be available: 9/17/2018
EDA60k	Android 7.1	(non-GMS) Upgrade to Android OS release 206.01.00.0018 or later Update ECP to version 2.30.00.0167 or later Release will be available: 9/17/2018

Product Name	Software	Status
EDA51	Android 8.1	Update to CommonES 6.02.01.4593 Release will be available: 9/17/2018

Mitigating Techniques

Honeywell recommends whitelisting of trusted applications to limit risk from malicious apps being installed on the device. Additional security recommendations are found in the Network and Security Guide for Honeywell Mobile Computers. (https://www.honeywellaidc.com/en/-/media/en/files-public/technical-publications/multi-product/ALLSKU-AND-ENUS-ZY.pdf)

Acknowledgment

Honeywell would like to acknowledge Google's Android Team for reporting this vulnerability. No public announcements or malicious use of the vulnerability described in this advisory is known.

Product Support

For assistance with this vulnerability please contact Honeywell through your product support channel. If you become aware of a vulnerability or other security concern involving a Honeywell product, please notify Honeywell by sending an email to security@honeywell.com

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS