Honeywell

CYBER SECURITY UPDATE

Honeywell Safety and Productivity Solutions
Qualcomm Hexagon SDK and cDSP vulnerabilities

Publish Date: 08-14-2020

Reference: Check Point Software Technologies, “Achilles: Small chip, big peril”

CVEs: CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 and CVE-2020-11209

Severity: Some are High depending on usage

Summary

The compute digital-signal processor (DSP) is a subsystem of the Qualcomm™ snapdragon system-on-module that allows the mobile device to process simple sets of data and perform high performance operations using low power. Researchers at the Defcon 2020 security conference have presented vulnerabilities within the Hexagon SDK which allows applications access to the cDSP, and potentially perform malicious actions. The primary impact of these vulnerabilities is the potential for remote code execution and denial of service (DoS), potential buffer overflow and crashing of essential system processes.

Qualcomm will be releasing a patch for these issues in two parts as follows:

- Part 1 of the patch will fix 5 separate issues with how the Hexagon SDK accesses to the cDSP. Along with part 1 of this fix, customers are encouraged to limit any application access to the DSP via application whitelisting while we wait on part 2 to be released. Honeywell has already integrated this first part of the patch in the MR25 release for Android™ O and in Android N as part of the MR21 release for the products supported below. Honeywell expects to release part 1 of the patch for Android P in MR09 expected on August 31, 2020.
- Part 2 of the patch that will fix the remaining issues with the compute-DSP will be released later by Qualcomm and incorporated by Honeywell as soon as possible. Qualcomm has not specified a definitive date for when this second part of the patch will be released. Honeywell will keep our customers updated via notice and standard support channels.

Honeywell Safety and Productivity Solutions
300 S. Tryon St Suite 500
Charlotte, NC 28202
800-582-4263
www.honeywellaidc.com

Honeywell

CYBER SECURITY UPDATE

Recommended Action

Honeywell will release firmware software updates to include security fixes as these are made available by our partner and specified in the following table. The following list contain those products that Honeywell has identified as potentially affected by this vulnerability. Updates will be made available at https://hsmftp.honeywell.com, or through your Honeywell product support channel.

Product Name	Software	Status	Comments
Thor VM1A	All OS versions	Affected	Android O MR25 includes part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of the patch is expected by December 31, 2020
Thor VM3A	All OS versions	Affected	Android O MR25 includes part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of the patch is expected by December 31, 2020
CK65	All OS versions	Affected	Android O MR25 includes part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of the patch is expected by December 31, 2020
CN80	All OS versions	Affected	Android O MR25, and Android N MR21 include part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of patch expected December 31, 2020
CN80G	All OS versions	Affected	Android P expected on August 31, 2020. Part 2 of the patch is expected by December 31, 2020
CN85	All OS versions	Affected	Android O MR25 includes part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of the patch is expected by December 31, 2020
CT40	All OS versions	Affected	Android O MR25, and Android N MR21 include part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of patch expected December 31, 2020
CT60	All OS versions	Affected	Android O MR25, and Android N MR21 include part 1 of patch, Android P MR09 expected on August 31, 2020. Part 2 of patch expected December 31, 2020
EDA60K	All OS versions	Affected	Android N MR25 expected on December 31, 2020
EDA51	All OS versions	Affected	Android O MR28 expected on December 31, 2020
EDA71	All OS versions	Affected	Android O MR11 expected on December 31, 2020
EDA61K	All OS versions	Affected	Android P MR18 expected on November 31, 2020

Mitigating Techniques

Honeywell recommends customers whitelist only the applications needed for users' workflow in order to block all others that could take advantage of this vulnerability to access the cDSP and perform malicious operations.

Additional security recommendations are found in the Honeywell Mobile Computers Network and Security guide for Android Operating systems.

Honeywell Safety and Productivity Solutions
300 S. Tryon St Suite 500
Charlotte, NC 28202
800-582-4263
www.honeywellaidc.com

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

Honeywell Safety and Productivity Solutions
300 S. Tryon St Suite 500
Charlotte, NC 28202
800-582-4263
www.honeywellaidc.com