Honeywell
THE POWER OF CONNECTED

Cyber Security Update

Kr00k Vulnerability Notification

Publish Date: 03-03-2020
CVSS v3.0 Base Score: 3.1
Reference: Eset Kr00k Web site https://www.eset.com/int/kr00k/

CVE: CVE-2019-15126

Summary

At RSA 2020, security researchers presented an exploitable condition (i.e. vulnerability) recently discovered in Broadcom or Cypress WiFi Chipsets. This security vulnerability impacts WiFi connections using WPA2-Personal or WPA2-Enterprise with AES-CCMP encryption. Fortunately, a threat agent will need to be physically located to the vulnerable device and the connected Wireless Access Point (WAP). Once the vulnerability is exploited, the threat agent is able intercept and decrypt wireless network traffic.

Honeywell is not aware of any Honeywell Productivity Products currently affected. The “Mobility-Edge” mobile computers are not affected.

To date, there are no known exploits in-the-wild. Neither are active monitoring of threat intelligence sources indicating active threats.

Recommended Action

RECOMMENDED ACTION

Honeywell Safety & Productivity Solutions strongly recommends customers work with their respective service teams to undertake preventative measures to improve the security of their systems, including the following:

- **Security Updates**: The corrective action will be to install updates to affected devices as/when they become available. See Affected Products List for Patch Availability.
- **Wi-Fi Usage**: Until patches are available, continue to use WPA2 encryption as it is believed to be safer than alternative Wi-Fi security options. Avoid the use of public Wi-Fi services. If public Wi-Fi must be used, utilize a Virtual Private Network (VPN) connection to enhance the security of your network traffic.
- **Anti-Virus**: Always ensure that anti-virus software is up to date and installed across all assets.
- **Keep Current**: Unpatched or outdated operating systems and application software are often more susceptible to cyber-attacks, ensure updates are being installed on a timely and regular basis.
- **Backups**: Ensure appropriate backups and system restoration procedures are in place, with copies of the most recent backup stored in an offline/disconnected state to reduce infection susceptibility.

Mitigating Techniques

Honeywell recommends, as a mitigating control to ensure to update the firmware of your Wireless Access Points (WAPs) are updated from your manufacturer. As long as your WAPs are properly patched for this vulnerability, forcing disassociation to perform this exploit should make it harder for an attacker.

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

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