Honeywell
THE POWER OF CONNECTED

Cyber Security Update

Security Notification – Wi-Fi Vulnerability (KRACK) from Safety & Productivity Solutions

BACKGROUND

Security researchers have discovered a flaw in the commonly used wireless network security protocol (WPA2) which may allow an attacker to compromise and/or gain unauthorized access to wireless devices and networks. The vulnerabilities are in the WPA2 protocol, not within individual WPA2 implementations, which means that all WPA2 wireless networking may be affected. Mitigations include installing updates to affected products and hosts as they become available from manufacturers. These vulnerabilities go by the name 'Key Reinstallation Attacks or 'KRACK'. For more details on the vulnerability specifics see the industry links below.

RECOMMENDED ACTION

Honeywell Safety & Productivity Solutions 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. Contact Honeywell Technical Support to obtain software updates.
- **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.

ADDITIONAL RESOURCES

- Vulnerability Note VU#228519
  https://www.kb.cert.org/vuls/id/228519
- WPA2 Key Reinstallation Attacks
  https://www.krackattacks.com

AFFECTED PRODUCTS – 01 Dec 17 Updates In Bold

Productivity Products	
Mobility – Honeywell Supplied Supplicant	
Product Name	Patch Availability
Android (Nougat & Marshmallow)	
Dolphin CT50/Dolphin 75e	**M Available - KK 29 Dec 17**
CN51	**M Available - JB Upgrade**
CN75, CN75e, CK75	**Available**
EDA 50, 60, 70	**Available**
Windows*	
CN51	**Available**
CN75, CN75e, CK75	**Available**
Dolphin CT50/Dolphin D75e	**Win10 - Available** **Win8.1 - Upgrade to Win10**
Thor VM3, VM2	**Win10, Win7, CE6 - Available**
Thor VM1	**WES 2009 - Upgrade** **CE 6 - Available**
CV31	**Available**
D99 Series	**Available**
CK3R, CK3X	**Available**
CN70, CN70e, CK70, CK71	**Available**
Tecton	**Available**
D6110, D6510	**Available**
D70e	**Available**
D60s	**Available**
D7800, D9700	**Available**
Printers	
Performance	**Not Affected**
A, H, M Class	**5 Feb 18**
E, I Class	**10 Jan 18**
LP3	Pending
MF2Te, MF4Te	Pending
OC2, OC3	Pending
PB22, PB32, PB50	**20 Jan 18**
PC43d, PC43t, PD43, PD43c	**22 Feb 18**
PD42, PD42D	**8 Jan 18**
PM43, PM43c, PM23c	**2 Feb 18**
PR2/PR3	**17 Jan 18**
PR2/PR3 IOS	**17 Jan 18**
PrintPAD CN3, CN4,CN3e, CN4e, CN51,CN51e, CN70 Series	Pending
PrintPAD MC65/67, MC70/75	Pending
PX4i,PX6i	Pending
RL3e, RL4e WLAN	**17 Jan 18**

* Microsoft Zero Configuration is pending