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.
- **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 – 20 OCT 2017

Productivity Products	
Mobility	
Product Name	Patch Availability
Android (Nougat & Marshmallow)	
Dolphin CT50	20 Nov 17 - KK Pending
Dolphin D75e	30 Nov 17 - KK Pending
CN51	30 Nov 17 - JB Pending
CN75, CN75e, CK75	30 Nov 17
EDA 50, 60, 70	30 Nov 17
Windows	
CN51	Pending
CN75, CN75e, CK75	Pending
CT50	Win10 - 10 Nov 17 Win8.1 - Pending
Dolphin D75e	Win10 - 10 Nov 17 Win8.1 - Pending
Thor VM3, VM2	Win10, Win7, Wes7 - 10 Nov 17 Wec7, CE6, Wes2009 - Pending
Thor VM1, CV31	Pending
D99 Series	Pending
CK3R, CK3X	Pending
Cx70 Series	Pending
Tecton	Pending
D6110, D6510	Pending
D6510	Pending
D70e	Pending
D60s	Pending
D7800, D9700	Pending
Printers	
Performance	Pending
A, E, I, H, M Class	Pending
LP3	Pending
MF2Te, MF4Te	Pending
OC2, OC3	Pending
PB22, PB32, PB50	Pending
PC43d, PC43t	Pending
PD43, PD43c	Pending
PM42, PM42D	Pending
PM43, PM43c, PM23c	Pending
PR2/PR3	Pending
PR2/PR3 IOS	Pending
PrintPAD CN3, CN4,CN3e, CN4e, CN51,CN51e, CN70 Series	Pending
PrintPAD MC65/67, MC70/75	Pending
PX4i,PX6i	Pending
RL3e, RL4e WLAN	Pending
J59	Pending