MEDIA RELEASE - For Immediate Release
17 October 2017

Wi-Fi Vulnerability Highlights Need for Innovation

Significant change is required to the way we consider digital security following the announcement overnight of the Key Reinstallation Attack (KRACK) vulnerability in the Wi-Fi Protected Access 2 (WPA2) security protocol. The vulnerability identifies a weakness within WPA2 that allows interception of traffic and insertion of malicious data into all wi-fi based communication.

The threat is to nearly all Wi-Fi based hardware, and there is currently no widespread fix to the problem. While the potential for personal information to be intercepted at the individual and home user level is significant, the impact on enterprise and integrated networks poses a far greater risk.

The nature of the vulnerability calls into question the suitability of a network standard like wi-fi for applications where monitoring and active security measures are not in place or possible.

“This vulnerability reinforces our belief that there is a need to change the approach to networks. Vulnerabilities will always be discovered, but the ability of the network to identify and respond to an attack or interception is vital.” Rollercoaster Digital Founder and Co-CEO, Andrew Snell said.

“We have long held the view, and have been working to create, a network protocol that self maps, diagnoses and amputates an infected point as necessary. We see it as the only way to adequately protect people and data, particularly in widespread IoT environments.”

The announcement of this vulnerability will have widespread impacts on wireless policies, while a fix is developed and rolled out. Organisations without an understanding of their network environment and what may be exposed if they were victim to an attack should familiarise themselves immediately.

“Internally, we will continue our cable-first policy for all work associated with personal or sensitive information. Until the full extent of the threat is known, we recommend using cabled networks where possible. It’s important to remember though, anyone looking to exploit your

network needs to be within range of it, it can't be done remotely. If you keep your wi-fi to the smallest area possible, your risk will be greatly reduced.

"We have no projects this actively impacts beyond the use of a user's personal device. Our services have additional security and certificate layers to protect user data." Mr Snell said.

The impact this vulnerability will have on product development and user behaviour will become more clear in the coming weeks. Rollercoaster Digital's approach incorporates network vulnerability into assessments and specifications.

"We call on the development and product community to work together to protect users on this issue - through collaboration and unified approach we can minimise the risk to people and their livelihoods." Mr Snell said.

If any organisation or individual has concerns about their current position and the threat posed to their products or productivity, they should make contact with a product or development company as soon as possible.

"This highlights as clearly as anything how quickly we need to move, and that we need to innovate on all fronts at the same time to ensure we have the best, most efficient, most secure technology."

- ENDS -

For more information or to arrange an interview please contact the Rollercoaster Digital team at media@rollercoasterdigital.com or call 0407 913 353

If you would like to discuss your current position and what it means to your business please contact the product support team at info@rollercoasterdigital.com or call 1800 800 005

About Rollercoaster Digital

Rollercoaster Digital is an Australian technology company headquartered in Canberra, developing a suite of products and technologies that connect people, devices and places. It also operates rcd.tech, a partner rapid prototyping and development program to assist large organisations, government and other start-up companies grow their own capability and reach market quickly.