What is the issue?

A number of security vulnerabilities were recently found to affect Ruckus Unleashed access points (APs). Collectively, these vulnerabilities allow an attacker to perform the following actions:

• Unauthenticated, remote code executions and unauthorized command line interface (CLI) and shell access
• Command injections
• Causing an AP to reboot by overflowing its software stack space
• Unauthenticated arbitrary file writing
• Server-Side Request Forgery (SSRF)

Under what conditions is my home network subject to the identified vulnerabilities?

It is important to understand that these vulnerabilities can only be exploited if an attacker is physically on premise and connected to your home Wi-Fi network. To connect to your Wi-Fi network, the attacker must know your Wi-Fi password.

Ruckus APs deployed in Lennar Homes cannot be remotely accessed because:

(a) The attacker may not know your network's public IP.
(b) Even if an attacker discovers your network's public IP, the Internet Service Provider (ISP)'s gateway typically blocks the SSH access to your network. This means that a remote attacker cannot gain access to your home network.

Should I take any action?

As a precautionary measure, we strongly recommend that you upgrade your home network to the latest 200.7 version (200.7.10.202.94) that is available on Ruckus Networks' site. You can upgrade with your mobile app or use a web browser by logging in to your Unleashed network (https://unleashed.ruckuswireless.com). Please note that you must be connected to your Wi-Fi network to upgrade with a web browser.

Ruckus Support
The Ruckus Networks Customer Services & Support organization can be contacted via phone, chat, and through our web portal. Additional details are available at https://support.ruckuswireless.com/contact-us

Phone: 855 782 5871 (or) 855 RUCKUS1