Honeywell

July 25, 2014

For Honeywell Security Group Dealers:

Information on Recent Media Coverage of Claimed Vulnerabilities in Wireless Security Systems

Recently, several stories have appeared in the media highlighting concerns about wireless security systems and their vulnerability regarding certain types of attacks. The information below will explain the issue and help answer questions that you may have or that you may receive from your customers.

- **What is Honeywell's position on the recent media coverage of claimed vulnerabilities in wireless security systems?**
  Honeywell security systems meet or exceed industry standards and include a variety of protections, such as available encryption, tamper resistance and jamming detection, which when employed significantly improve security. We are not aware that any homeowner's system has been affected by this potential vulnerability. Honeywell is committed to ensuring the security of our products and we are aggressively investigating the matter. Wireless transmissions by their nature are subject to potential risks. Honeywell will work through its dealer network to take any necessary remedial actions should our investigation deem it necessary.

- **It was represented that there are potential vulnerabilities in Honeywell wireless security systems. What are the specific vulnerabilities?**
  The article referenced the ability of a hacker to potentially intercept and interfere with wireless transmissions from a security system's sensors, and to jam those signals in order to suppress an alarm.

- **How would this attack work?**
  It was reported that the researcher utilized specialized equipment that transmits signals at the same frequency as the security system to disrupt ("Jam") the normal operation of the system. Additionally, the researcher further indicated that he could record and replay certain transmissions which could be used to send false signals from individual transmitters. We are aggressively investigating the matter.

- **How serious are these vulnerabilities?**
  We believe the referenced vulnerabilities present a low risk to homeowners. This sort of attack would require a person with sophisticated equipment and specific knowledge to exploit, as well as knowledge of the nature of the homeowner's system. We are not aware that any homeowner's system has been affected by this potential vulnerability.

- **How is my system protected from such an attack?**
  Honeywell security systems meet or exceed industry standards, and include a variety of protections, such as available encryption, tamper resistance and jamming detection, which when employed significantly improve security.

- **You mention that Honeywell security systems have Jamming Detection. How do we know if a customer's panel has jamming detection enabled, and if not, how do we enable it?**
  Every Honeywell wireless-ready security system includes a UL listed RF Jamming detection feature. If enabled by the dealer at install, the feature sends a trouble signal to the monitoring station should the wireless receiver be jammed by an unauthorized transmission. Direct Wire #161 (included with this packet) outlines how to enable jam protection on popular Honeywell panels.

- **Why does the jam protection feature have to be enabled by a dealer?**
  The common industry practice is to permit dealers to determine whether it is appropriate to enable the jamming protection in sensing devices. In certain instances where there is significant ambient wireless transmissions, the jamming detection may periodically trigger false attempted jam reports, which may distress resources from local authorities and first responders and, create a sense of complacency at home which may result in ignoring a real alert.

- **The security researcher says he can defeat the security system's jam protection – is that true?**
  We recently learned of this potential vulnerability and are aggressively investigating the matter. We will work through our dealer network to take any necessary remedial actions should our investigation deem it necessary.

- **You mention that Honeywell security systems offer encryption. Which devices offer encryption?**
  Honeywell offers encrypted Keyfobs, as those are the devices most directly associated with arming and disarming your security system. Most current Honeywell KeyFobs (5834-4 & variants) and all current Honeywell security panels support a 64-bit rolling-code encryption scheme. Honeywell recommends enabling encryption for all KeyFob devices which support it. See Direct Wire #161 (included with this packet) for additional details.

- **We utilize other vendors who claim to offer compatible 5800 sensors with Honeywell panels. Does this vulnerability pertain to those devices?**
  Honeywell cannot guarantee the security of non Honeywell sensors used with Honeywell Panels. You will have to contact the manufacturer directly for further information on their equipment.

- **My system uses cell-phone signals to communicate with the central station. Is that communication path at risk?**
  Honeywell cellular communications provide dual path transmission (GPRS with an SMS rollover backup), and iGSM communicators provide a wired IP as well as the two cellular data paths, providing three levels of redundancy. Additionally, Honeywell cellular and IP communications are strongly encrypted (256-bit AES cipher) which ensures security of communications.

- **My Honeywell security system is wired – do I have this vulnerability?**
  The potential vulnerability *only* affects security systems using wireless transmitters.

- **Does this vulnerability affect other connected home products, like a thermostat?**
  No, this potential vulnerability does not affect other Honeywell connected home products.

- **How can I tell if my security system has been compromised or tampered with?**
  Honeywell wireless transmitters have tamper detection features to detect and report physical tampering attempts. Wireless devices are supervised by the security system for physical tampering, and each follows a schedule of "check ins" with the system; if the transmitters don't check in on schedule, the system reports this to the monitoring station (and reports this locally on screen or keypads.) If jamming detection is enabled, the system sends a trouble signal to the monitoring station should the wireless receiver be jammed by an unauthorized transmission, the system also documents the trouble in its internal event log, and reports this locally on screen or keypads.

- **What is Honeywell doing to mitigate this problem in the future?**
  Honeywell is committed to ensuring the security of our products and we are aggressively investigating the matter. Immediately upon being made aware of this potential vulnerability, Honeywell began testing to understand the claims and will work through our dealer network to take any necessary remedial actions should our investigation deem it necessary.

- **Who should I contact if I have additional questions**
  Should you have any further questions please contact Honeywell Technical Support.