



FOR IMMEDIATE RELEASE

Garrett Response to Gizmodo Hacking Article

Garland, Texas (December 30, 2021) —Texas-based Garrett Metal Detectors today issued an official response to an online periodical which recently released an article regarding security products.

On December 21, 2021, the design, technology, and science website Gizmodo published an article by Lucas Ropek entitled "Walk-Through Metal Detectors Can Be Hacked, New Research Finds". A subtitle added "Garrett Metal Detectors, which are used in schools and government buildings, have security vulnerabilities that can be remotely exploited".

The response issued by Garrett is that Mr. Ropek used a sensational title to drive interest in his article. While perhaps that is to be expected, the content of the article omits important, relevant information in order to cast doubt on the integrity of checkpoint security installations. Had Garrett been given a reasonable amount of time to respond to Mr. Ropek's request for information, the Company would have requested to include the following pertinent information:

1. Garrett's walk-through metal detectors have been protecting the public since 1984 with no known incidents of hacking.
2. Fewer than 1% of Garrett's installed base of *PD 6500i* and *MZ 6100 (Multi Zone)* detectors includes a network integration accessory (a Garrett CMA or IC Module), and thus are not susceptible to the reported vulnerability.
3. Many customers who have purchased these accessories use them for data collection in a manner in which they are not connected to any type of network. These are not vulnerable to hacking.
4. Those customers who do connect the devices to a network typically employ robust firewall technologies to isolate connected devices from potential hackers.
5. The WiFi protocols in the wireless versions of the integration accessories use robust data encryption to prevent intrusion into the network.

6. The only Garrett detectors that have any level of risk of hacking are the ones that both include the network integration accessory and are connected to a user's unprotected network.
7. The vulnerabilities identified by Cisco that were mentioned in the article were addressed by a Garrett software update to the CMA and IC Module accessories before Mr. Ropek's article was published and the effectiveness of those fixes have been certified by Cisco to be effective.
8. Garrett's CMA and IC Module software update is currently available for customers who need it. Please contact Garrett technical support at security@garrett.com or by calling Garrett at 1 800-234-6151.
9. The operating systems and software on the *PD 6500i* and *MZ 6100* are isolated from the IC Module and can only be updated through physical access to the hardware. Remote firmware updates for the *PD 6500i* and *MZ 6100* are not supported.

About Garrett Metal Detectors

Garrett Metal Detectors, co-founded by electrical engineer Charles Garrett and fourth generation educator Eleanor Smith Garrett, is the global leader of metal detection products for security and law enforcement applications worldwide. For more than 57 years, Garrett has engineered the most advanced metal detection products, including walk-through, hand-held, and ground search metal detectors for the security industry. Garrett is an International Standards Organization (ISO) 9001:2015 certified company.

Related Link: www.garrett.com

Contact Person: steve.moore@garrett.com