Date: January 10, 2017

To: Germany Distribution

PowerG & PowerCode
Radio Protocols
Security at Its Best

Scope of Problem

On November 23rd a research article was published in PlusMinus magazine on TV station ARD, showing the ability to neutralize security systems by tapping into the radio transmission using a simple radio scanner and reproducing the same transmission to disarm the security system when home and business owners are away.

None of the tested units in this research were from Visonic.

PowerG Status

Visonic PowerMaster panels communicate using PowerG™ technology, a tree-topology radio protocol that was developed especially for security applications and designed to provide both operational and security advantages.

From an operational perspective, this radio provides a very long transmission range with low energy consumption so that the installation process is simplified and the battery life expectancy of devices is longer than industry standards.
From a security perspective, the PowerG technology is a synchronised radio with frequency hopping and strong time-relay 128-bit AES encryption mechanism making **PowerG immune to such scanners and radio signal reproduction tools.** Even if an intruder overcomes the frequency hopping (not an easy task) and then replays it, the panel will have already discarded the radio frequency message and moved on to the next, making it virtually impossible to disarm or jam.

**PowerCode Status**

Visonic PowerMax panels use PowerCode radio technology. When disarming the system via wireless keyfob, a CodeSecure™ digital sequence is transmitted and identified by a compatible CodeSecure™ receiver and a 4-bit function code is sent.

On the next operation a different digital sequence is transmitted that differs from the one previously used and following the same process. As a result, malicious “code grabbing” is virtually impossible.

**Conclusion**

All Visonic panels use either PowerG or PowerCode radio protocols, and are immune to threats as shown on PlusMinus Magazine.