Vulnerability Disclosure

Maintaining the security of our networks is a high priority at Squire. The security researcher community regularly makes valuable contributions to the security of organizations like ours and the broader Internet, and Squire recognises that fostering a close relationship with the community will help improve our own products and services. So if you have information about a vulnerability in one of our products or services, we want to hear from you!

We are interested in hearing about any vulnerability or attack vector in any of our Inigma products and the supporting systems. This includes all our Inigma retail and commercial lock products, the supporting mobile applications and the web services and web sites that support them.

When submitting a vulnerability report please bear in mind the following:

- Well-written reports in English will have a higher chance of being accepted.
- Reports that include proof of concept code will be more likely to be accepted.
- Reports that include only crash dumps or other automated tool output will most likely not be accepted.
- Reports that include products not on the covered list will most likely be ignored.
- Include how you found the bug, the impact, and any potential remediation.
- Any plans for public disclosure.

What you can expect from us:

- A timely response to your email (generally within 5 business days).
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- An expected timeline for patches and fixes (usually within 120 days).
- Credit after the vulnerability has been validated and fixed.

At Squire we value your input. Henry Squire & Sons pledges not take legal action against researchers so long as they adhere to this policy.