Vulnerability Disclosure Policy

1. Introduction

Chameleon Technology (UK) Ltd, (Chameleon), is a leading energy technology company providing real time smart meter data and insights from connected devices. We are committed to the safety and security of consumers' data. To aid in this goal, we observe a formal Co-ordinated Vulnerability Disclosure approach to encourage constructive and co-operative relations with any security researchers and professionals who discover such concerns. We hope to foster an open partnership with the security community, and we recognise that the work the community does is important in continuing to ensure safety and security for all of our end users.

Chameleon goods are provided to the home through a number of different customers and partners. Where a report relates to those partner services, we may refer you to their support teams rather than our own.

We value the contributions of security community experts as essential for the growth and maturation of our products and services, and actively encourage their continued support. If you have reached this document as part of any other type of enquiry please use the provided contact mechanism on other parts of the website.

2. Scope of this policy

This policy is for security research professionals with reason to report a discovered vulnerability in Chameleon's products or services which may result in the compromise of consumer data and sets out the terms and expectations as part of our co-ordinated approach. We are in the process of broadening and improving coverage of products, and currently support resolution of vulnerabilities relating to models deployed in a SMETS2 smart metering environment and those connected to our supporting cloud services. Products and services designed and produced prior to the publication of this policy are not to be considered. Please note, all manufactured devices are marked with a year of manufacture.

3. Reporting

We will accept vulnerability reports on our products outside of the scope outlined above, but the response and resolution processes may not be conducted in the same way.
We maintain a list of known vulnerabilities and may share details of known vulnerabilities, where relevant to a submission. This is to cover repeat submissions of issues and allow potential submitters to reflect on whether the issue is relevant and the published resolution if not.

Reports may be submitted here.

4. Legal Action

Chameleon Technology (UK) Ltd will not look to take legal action over vulnerabilities where the researcher has actively and responsibly engaged with us in compliance with this policy and by keeping matters confidential throughout the resolution process. Responsible engagement relies on our code of ethics being followed by the researcher. In cases which involve other vendors or companies, it may be necessary for a third-party arbitrator or co-ordinator to become involved in the resolution of a report. In such cases, these terms will be preserved.

5. Confidentiality

In order to protect our end-users, we request that you not release Information about a potential vulnerability to any third-party until we have researched, responded to, and addressed the reported vulnerability or agreed to the timing and scope of such a release. In like manner, we will keep all information confidential throughout the resolution process.

It is expected that researchers submitting vulnerabilities follow an ethical approach to their work. Our code of ethics is available for you to review here.

6. Vulnerability Reporting Requirements

When reporting a vulnerability to us please include the following information in your submission:

- Contact details for the originator. Please include an email address and full name (Options for address and company information URL name of insitution.)
- Where the report relates to a product:
    - The model and serial number
    - Other connected equipment
    - Firmware version
- Where the report relates to a service Depending nature of your report, we aim to provide:
    - The service domain (URL)
    - Whether this relates to a cloud or web service
- The type of issue
- Include how you found the bug, the impact and any potential suggested remedy
- Submit in English. A well written description of the issue is more likely to be accepted
- Proof of concept code will be more likely to be accepted
- Reports should be kept to only relevant data and information. Submissions that include only crash dumps or other automated tool output will most likely not be accepted
- Reports that include products produced prior to the adoption of this policy are not covered by it. Where possible though, we will endeavor to meet the same terms.
- As stated previously, we expect you to keep matters confidential until we agree publication of any information.
- In response to your report, Chameleon will provide:
- A response within 3 business days of the submission.
- An open, responsive dialogue to discuss issues.

Depending nature of your report, we aim to provide:

- For known vulnerabilities, references to relevant documentation.
- Notification when the vulnerability analysis has passed each stage of our vulnerability analysis.
- An expected timeline for any patches, fixes or updates.
- First finder credit to the researcher after the vulnerability has been validated and fixed.

7.Appendix A: Code of Ethics

a. Before and during ethical hacking, determine the sensitivity or confidentiality of the information involved. This should ensure that you do not violate laws, rules and regulations in handling sensitive personal, financial or proprietary information.
b. During and after ethical hacking, maintain transparency with the company. Commu-nicate all relevant information you found while ethically hacking the company's system, net-work or device. Transparency ensures that the company knows what is going on. Transpar-ency enables the company to take necessary actions for security of the system or network.
c. While performing ethical hacking, do not go beyond the limits set.
d. After performing ethical hacking, never disclose resulting information to other parties unless agreed with the company. Ensure the protection of the company. Ethical hacking is done for the security of the device, system or network. Disclosure of confidential information renders ethical hacking ineffective. Private information must be kept private, and confidential information must be kept confidential.