Vulnerability Disclosure Policy
for Connected Products

Introduction

Since security is of critical importance to us and to our customers, we at CAME SpA are committed to ensuring the safety and security of our products and services. CAME SpA supports coordinated vulnerability disclosure and encourages responsible vulnerability testing, we take any reports of potential security vulnerabilities seriously.
To report a potential security vulnerability, please follow the steps described in the "Reporting procedure" section.

Reporting procedure

- Submit the Vulnerability Report at security.iot@came.com.
- Use our PGP public key *https://www.came.com/global/securityiotpublickey* to encrypt any email submissions.
- Write the Vulnerability Report in English.
- Provide sufficient contact information, such as:
    a. your email;
    b. name of the person who found the vulnerability.
- Provide information about the vulnerability:
    a. date when the vulnerability has been detected;
    b. details about how it has been discovered;
    c. a technical description of the vulnerability.
- Provide as much information as you can on the product or service affected by the vulnerability, like:
    a. version number (hardware and software);
    b. configuration of the setup used.
- If you wrote specific proof-of-concept or exploit code, please provide a copy. Please ensure all submitted code is clearly marked as such and is encrypted with our PGP key.
- If you have identified specific threats related to the vulnerability, assessed the risk, or have seen the vulnerability being exploited, please provide that information.

Internal assessment and action

1. CAME SpA will acknowledge receiving your Vulnerability Report within 3 business days
2. If the Vulnerability Report contains all the required information, CAME SpA will provide a unique tracking number and a contact person;
3. If the Vulnerability Report is not complete (more information is needed), CAME SpA will request you the missing information, and no more action will be taken.
4. CAME SpA will start an internal Vulnerability Management Process to manage the reported vulnerability:
   ○ Vulnerability Identification;
   ○ Vulnerability Triage;
   ○ Vulnerability Assessment;
   ○ Vulnerability Addressing.
5. CAME SpA will monitor the status of the Vulnerability Management Process, and you will receive a communication at the end of each stage.
6. CAME SpA will use existing customer notification processes to manage the release of patches or security fixes, which may include without limitation and at CAME SpA's sole discretion, direct customer notification or public release of an advisory notification on our website.
7. If the vulnerability is actually in a third party component or service which is part of our product/service, CAME SpA will notify the Vulnerability Report to that third party and advise you of that notification. To that end, please inform us in your email whether it is permissible in such cases to provide your contact information to the third party.

Notice

If you share any information with CAME SpA in the context of responsible disclosure, you are agreeing that the information you submit will be considered as non-proprietary and non-confidential.
CAME SpA is allowed to use shared information, or part of it, without any restriction. You agree that submitting information does not create any rights for you or any obligation for CAME SpA. Personal data is processed by CAME SpA based on the privacy policy
https://www.came.com/global/en/privacy-policy.

CAME S.p.A.
Sede Legale e Operativa:
Via Martiri della Libertà, 15
31030 Dosson di Casier (TV) - Italy
T +39 0422 49 40

Sede Operativa:
Via Cornia, 1/c
33079 Sesto al Reghena (PN) - Italy

Cap. Soc. € 1.610.000,00 i.v.
C. F. / P. I. 03481280265 - VAT IT 03481280265
REA TV 275359 - Reg. Imp. TV 03481280265
came@pec.came.com - info@came.com - **www.came.com**