VULNERABILITY DISCLOSURE POLICY

Purpose

The objective of this Policy is to define what we are expecting from a security researcher when reporting a security vulnerability, and what we will do in response.

Scope

This vulnerability disclosure policy applies to BB Energy's external interested parties who are considering reporting a technical security vulnerability. Please read this vulnerability disclosure policy before you report a security vulnerability and always act in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting security vulnerabilities

If you discover a technical security vulnerability relating to BB Energy's information systems, please submit your report to the following email address, it@bbenergy.com.

In your report please include details of:

- When the vulnerability was detected;
- The IP address, website or website page where the vulnerability was detected;
- If the vulnerability results to a remote code execution (RCE) or allows access to information systems;
- A brief description of the type of vulnerability, for example; “SQLi, XSS, CSRF, Malformed request, attrition, etc.”;
- Steps to reproduce the vulnerability.

Unfolding the process

After you have submitted your report, we will respond to your report within 7 working days and aim to triage your report within 14 working days. We’ll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity, and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected parties, so please do continue to coordinate public release with us.

Rules of engagement

Security researchers must not:

- Break any applicable law or regulations;
- Violate the privacy of BB Energy's users, staff, contractors, services, or systems;
- Access unnecessary, excessive or significant amounts of data;
- Modify data in BB energy's systems or services;
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities like fuzzers, amplifiers etc.
- Attempt or report any form of resource exhaustion denial of service;
- Disrupt BB Energy's services or systems;
- Social engineer, 'phish' or physically attack BB Energy staff or infrastructure;
- Demand financial compensation to disclose any vulnerabilities.

Security researchers must always:

- Comply with National and European data protection laws and regulations;
- Securely delete all data retrieved during security research as soon as it is no longer required or within 1 week of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

Legal Disclaimer

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give permission to act in any manner that is inconsistent with the law, or which might cause BB Energy or partner organizations to be in breach of any legal obligations.