**Mojaloop Vulnerability Reporting Procedure**

**Overview**

This procedure is for guiding the public on how security vulnerabilities should be reported safely and responsibly to the dedicated security team within Mojaloop. As representatives of the Mojaloop Community, we strongly encourage everyone to alert us of the potential security vulnerabilities privately first, before disclosing them in a public forum – a right everyone is entitled to without any permission whatever from us as the maintainer of the platform.

**Contacts**

A list of security contacts for Mojaloop projects is available. If you can't find a project specific security e-mail address and you have an undisclosed security vulnerability to report, then please use the general security address below:

1. [sam@modusbox.com](mailto:sam@modusbox.com)
2. [lewisd@crosslaketech.com](mailto:lewisd@crosslaketech.com)
3. [Victor.akidiva@modusbox.com](mailto:Victor.akidiva@modusbox.com)
4. [godfreyk@crosslaketech.com](mailto:godfreyk@crosslaketech.com)

Please note that the security contacts should only be used for reporting undisclosed security vulnerabilities in Mojaloop projects and managing the process of fixing such vulnerabilities. We cannot accept regular bug reports or other security related queries at these addresses. All mail sent to these addresses that does not relate to an undisclosed security problem in an Mojaloop project will be ignored.

NB. Security vulnerabilities should not be entered in a project's public bug tracker unless the necessary configuration is in place to limit access to the issue to only the reporter and the project security team.

The contacts listed above are intended to be used until the formation of a formal Organization for Mojaloop. Once such an entity is formed, an alias such as [security@mojaloop.io](mailto:security@mojaloop.io) or a similar will be provided, which will replace the existing list. This will however, be communicated to the Community.

**Reporting Format**

Please send one plain-text email for each vulnerability you are reporting. We may ask you to resubmit your report if you send it as an image, movie, HTML, or PDF attachment when it could just as easily be described with plain text.

**Vulnerability Types**

We have no restrictions whatsoever for the vulnerability type or method used to uncover the vulnerabilities. The public is welcome to use any methods or tools available to them, including analysis of the source, and apply any methodology of their own in finding vulnerabilities, provided that the vulnerability report is clear and self-descriptive.

**Advance Security**

We use standard TLS encryption in our mail systems however should the reporter requires additional layer security before sending the info then we are flexible to cater for that on a case by case basis by contacting [godfreyk@crosslaketech.com](mailto:godfreyk@crosslaketech.com)

**Vulnerability Information**

Further information regarding handling of published vulnerabilities for an Mojaloop project can usually be found on the project’s GitHub Account - insert a link. If you can't find the information you are looking for on GitHub, you should ask your question on the project's user mailing list above.

**Vulnerability Handling**

An overview of the vulnerability handling process is:

1. The reporter reports the vulnerability privately to Mojaloop.
2. The appropriate project's security team works privately with the reporter to resolve the vulnerability.
3. A new release of the Mojaloop package concerned is made that includes the fix.
4. The vulnerability is publicly announced to the Mojaloop Community

A more detailed description of this process will be made available soon to the public to provide full understanding of our internal handling process.

Here we have a gap to define this internal vulnerability handling process as a separate procedure from this public reporting one