

NETITUDE

INTELLIGENT CYBER SECURITY & RISK MANAGEMENT

Penetration Test Management Report





Penetration Test Management Report

Nettitude provides a wealth of knowledge, expertise and experience in regards to Data Security. We provide comprehensive vulnerability assessment, penetration testing and application assessment services. Our team of dedicated security consultants deliver best in class testing capability as well as strong remediation advice and guidance.



REPORT CONTENTS

1	Distribution List.....	4
	Nettitude.....	4
	The Linux Foundation	4
	Revision History.....	4
2	Executive Summary.....	5
	Background.....	5
	High Level Assessment.....	5
	Nettitude were able to.....	5
	Primary Security Concerns.....	5
3	Risk and Analysis	6
	Risk Profile.....	6
	How to understand the values below?.....	6
	How do we calculate risk?	6
	Risk and Priority Key	6
	The Linux Foundation Risk Details	7
	Overall Risk Status.....	7
4	System Analysis	9
5	Next Steps.....	10
	Post Engagement Actions.....	10

NETTITUDE

1 DISTRIBUTION LIST

Nettitude

Name	Title
Graham Shaw	Security Consultant
Kristopher Vasilik	Account Manager

The Linux Foundation

Name	Title
David Huseby	Security Maven, Hyperledger

Revision History

Version	Issue Date	Issued By	Comments
0.1	4 th April 2018	Graham Shaw	Initial Draft
0.2	10 th April 2018	Jose Lopes	Quality Assurance
0.3	10 th April 2018	Kristopher Vasilik	Quality Assurance
1.0	12 th April 2018	Graham Shaw	Final

The contents of this report belong to The Linux Foundation. They have been provided by Nettitude based on the work detailed within this report and were accurate at the time of testing. Nettitude presents no guarantee that the details in this report are a true reflection of the tested environment at the present time.

NETTITUDE

2 EXECUTIVE SUMMARY

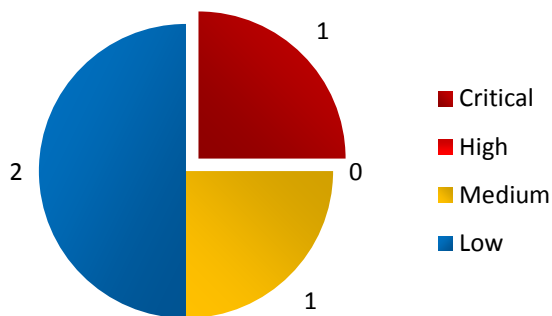
Background

The Linux Foundation engaged with Nettitude in February 2018 in order to assess the overall security posture of their Hyperledger Iroha software product.

High Level Assessment

Based on The Linux Foundation's risk profile, primary security concerns and the vulnerabilities identified at the point of the engagement, Nettitude have tentatively found Iroha to:

REQUIRE IMMEDIATE ATTENTION



Nettitude were able to...

- Sign an object multiple times using the same keypair, in a manner that Iroha is unable to distinguish from multiple signers.
- Cause memory to leak in a manner that would eventually result in denial of service.
- Show how IP addresses could be made permanently unusable by peers within an Iroha network.

Primary Security Concerns

Nettitude worked with The Linux Foundation, prior to this engagement, to investigate and understand the primary security concerns associated with the systems in scope.

These concerns are not exhaustive, but rather represent a method of helping to gauge the severity of the overall risk presented by the systems in scope.

Concern	Description	Data Category	Result
Access Control	Access should not be allowed unless the user has been authenticated and has appropriate authorisation	Confidentiality Integrity	FAIL
API Vulnerabilities	The API endpoints should not be vulnerable to exploitation	Confidentiality Integrity Availability	FAIL

Table 1 – The Linux Foundation Primary Security Concerns

NETTITUDE

3 RISK AND ANALYSIS

Risk Profile

Nettitude present the following high level risk profile for The Linux Foundation in order to help contextualise the reasoning behind each findings severity and the overall system rating of 'requires immediate attention'. This is Nettitude's own assessment, based on their knowledge and understanding of The Linux Foundation, as an organisation.

How to understand the values below?

All risks should be run through your own internal risk register and methodology. The aim below is to provide you with a benchmark and a stake in the ground. We have only had a glimpse of the data you hold, and have based the impact on your business on industry equivalents. It's very important that you re-assess and understand these values according to your business and its risk appetite.

How do we calculate risk?

In brief, assets have values which if compromised will have an impact on your business (reputation, ability to function, fines, etc). Weaknesses (or vulnerabilities) allow threats to access/disrupt these assets. The location of the vulnerability will determine the likelihood of the weakness to be exploited.

Risk is a factor of the vulnerability, the impact and the likelihood. Threats need to be considered, but these are outside the scope of this work (See [ISO31000](#) for a detailed methodology).



Risk and Priority Key

The following key shows how the level of risk and priority will be represented within this report.

Critical	
High	
Medium	
Low	

NETITUDE

The Linux Foundation Risk Details

The table below shows the values calculated for this environment.




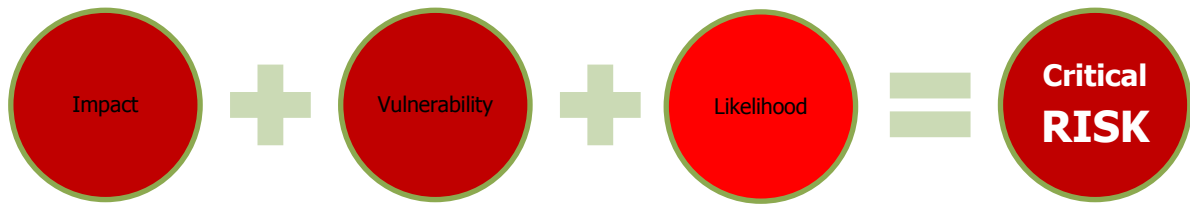
Risk Factor	Grade	Reasoning
Impact		Hyperledger Iroha is intended for use in high-risk, security-critical environments. In addition to managing valuable digital assets itself, if compromised it could act as a gateway to other high-value systems.
Vulnerability		<p>Blocks can be signed multiple times using the same keypair, in a manner which Iroha is unable to distinguish from multiple signers. If such blocks can be propagated (which has not been proved but seems likely), this would allow a rogue peer to unilaterally add blocks to the blockchain, thereby comprehensively undermining its integrity.</p> <p>Proposals can similarly be signed by multiple users. If the multi-signatory account feature was functional (which it was not at the time of testing), this would have allowed individual signatories to unilaterally authorise a transaction which ought to require multiple signatories.</p> <p>A memory leak was found which could potentially be used to cause a denial of service.</p> <p>Peers can only be added, and once added their public keys cannot be changed. Amongst other concerns this would allow IP addresses to be put permanently beyond use.</p>
Likelihood		<p>Multiple signing requires that the threat actor have possession of an authorised keypair, either for a peer or a user as appropriate. This requires either an insider or a two-stage attack. Neither is unachievable, and the stakes could be high, therefore likelihood is assessed to be high for blocks and medium for proposals.</p> <p>The memory leak would be of dubious utility to an attacker due to its low rate, even if the need for authentication were overcome. The likelihood of it happening is assessed to be very low. Similarly for putting IP addresses beyond use, due to the need for the CanAddPeer capability.</p>

Table 2 – The Linux Foundation Risk Breakdown

Overall Risk Status

The overall risk for the environment under review for The Linux Foundation is shown below:

NETTITUDE



The Linux Foundation may perceive their risk profile to differ from what is presented in this section, in which case Nettitude would be happy to engage and discuss.

NETTITUDE

4 SYSTEM ANALYSIS

Blocks should only be added to the blockchain when a supermajority of peers have voted that this should happen. These votes, in the form of signatures, are recorded in the blockchain, and they are checked when the blockchain is validated.

Unfortunately, Iroha does this on the basis that the number of distinct signatures attached to a block is equal to the number of unique peers which have signed it, the unstated assumption being that you can't have two distinct signatures for the same message and keypair.

This would be a correct assumption if the only way to generate compatible signatures was to use a standard implementation of the ed25519 signature algorithm on which Iroha relies. However, Nettitude was instead able to devise a modified (but compatible) algorithm which produces a different signature each time it is applied. There is no practical limit to the number of signatures that can be produced using a single keypair, therefore it is a straightforward matter to generate enough to form what appears (so far as the Iroha software is concerned) to be a supermajority.

If blocks signed in this way can be made to propagate throughout the network, a single rogue peer would be able to unilaterally add blocks to the blockchain, without first having to form a consensus. This would comprehensively undermine the integrity of the blockchain. In particular it would turn the distributed nature of an Iroha network from an asset into a liability (since any peer would be able to execute the attack).

Nettitude has confirmed that the signing algorithm works, and that Iroha treats the resulting signatures as both distinct and valid. A proof of concept has been demonstrated for a similar attack against multi-signatory accounts. This is sufficient for Nettitude to be very confident, at a minimum, that there is a serious weakness in the code which ought to be fixed.

In the absence of a working end-to-end demonstration, Nettitude is not yet fully confident that this vulnerability is exploitable. However, the available evidence points towards that being the case, and an initial discussion with a member of the Iroha development team reached the same conclusion.

A similar type of attack would have been possible against the multi-signatory account feature if it was functional (which it was not at the time of testing). This has been demonstrated to a high degree of confidence.

There is a slow memory leak in Iroha which could conceivably be used to mount a denial of service attack (although the number of transactions required would be very large).

Finally, Iroha has an 'add peer' command, which allows a peer to be added to the network with a given IP address and public key, but there is no way to reuse that IP address with a different key. This would allow an attacker with sufficient privileges to place any number of unused IP addresses permanently beyond use.

NETTITUDE

5 NEXT STEPS

Post Engagement Actions

Nettitude recommends that The Linux Foundation perform the following post engagement activities in the order of priority indicated.

Activity	Description	Priority
1 Debrief from Nettitude	Nettitude will deliver a formal debrief to The Linux Foundation in order to ensure that the findings of this engagement have been fully comprehended and to help assist in the formulation of a remediation plan.	
2 Multiple signing	Ensure that Iroha counts the number of distinct public keys used to sign an object, as opposed to merely the number of distinct signatures.	
3 Memory leak	Fix the memory leak which was identified.	
4 Peer registration	Ensure that the public key for an IP address can be changed.	

Table 3 – Post Engagement Activities

Nettitude recommend that the contents of this report are fully understood prior to progressing onto the technical report, which provides further information on the individual vulnerabilities identified, including how to fix them.