

# GETTY/IO

## Security Audit for: KleverChain

Version 0.1: August 30th, 2022



## About US

**Getty/IO** is an innovative remote IT security consulting firm that has the expertise to audit and recommendation to build secure web and mobile products. We specialize in modern Javascript technologies, lean and highly scalable backends, and blockchain technologies, which help to build the secure product for our customers worldwide.

Born in South America, GETTY has become the largest remote development firm in the region. We are a global company helping startups and enterprises from all around the world scale their development teams by providing them with the top remote developers and consultants:

- Blockchain - Security Review & Audit
- Smart Contract - Security Review & Audit
- Applications - Security Review & Audit

Our professionals are able to integrate to our Customer's teams and add value from day one. Agile methodologies, experience helping dozens of teams build products, and constant coaching and mentoring ensure all our engagements help our customers become successful.

In our hands, your entire process is safe, without the hassle, and as seamless as it can be. With the collaboration of our team of experts, you can expect to achieve much more. We are present in the United States, Canada, Portugal, Estonia, and Brazil.

## Abstract

Getty/IO has been appointed by the Klever Team to carry out the audit of KleverChain, his main blockchain. **Klever** is a decentralized p2p and self-custody wallet and **KFI** is the Klever blockchain governance token, to be used in Klever's blockchain parameters and kApp upgrades and the **KLV** token is the fuel of the blockchain, used to incentive people to participate in the blockchain thru stake as also pay networks fees"

This document presents the results of an Internal security audit for the KleverChain. This test aimed to identify security vulnerabilities that could negatively affect the systems under the scope, the data they handle, and consequently the business. They were simulated in a systematic way, attacks that were specifically tailored for the engagement's scope to test the resilience against real-life attack scenarios based on a black-box approach.

The analysis focused on vulnerabilities especially related to implementation, and on issues caused by architectural or design errors.

For each vulnerability discovered during the assessment, it was attributed a risk severity rating. The issue's severity classification is based on the potential it presents to provide means for fraud, data leakage, and other harmful events that may bring a direct adverse impact to the business.

## Methodology

Tests were conducted using risk factors, such as probability and impact. Each test and tool that has been used was focused on vulnerability's complexity and how it could be mitigated.

		IS Risk Vision		
Exploitation Complexity	Low	Medium	High	Critical
	Medium	Low	Medium	High
	High	Low	Low	High
		Low	Medium	High
		Impact		

## Tools and Vectors

The following tools and vectors were applied:

- Fuzzers: Bed, Rfuzz (Ruby), Sfuzz, fuzzing auxiliary modules of Metasploit, Spike (kit for developing fuzzers), etc.
- Brute force: John the Ripper, Hashcat, etc.
- Web applications: W3AF, Websecurify, Accunetix, Metasploit scanning auxiliary modules, CGI
- Scanner, ASP-Auditor, Oscanner, proxies such as Fiddler2 or WebScarab, Firefox browser plugins such as hacking toolbar, Tamper Data, User-Agent switcher, etc.
- Manual search in vulnerability repositories such as CVE, OSVD or NVD.
- Manual code analysis with the aim of finding weaknesses and developing bad practices, making use of editors, debuggers, and decompilers.
- Manual attacks: open port stress tests, SQL injections, CSS, RFI, overflows buffer detection, directory listing, web proxies (ZAP, Burp Suite, and webScarab), etc.
- Network communications analysis, Tshark, Ettercap, Wireshark, etc.
- In addition, this audit phase can be completed by using tools that automate the security analysis process of devices under studies, such as the well-known Nessus scanner and its GPL equivalent OpenVas.

## Tests Performed

### Information Gathering

- Conduct Search Engine Discovery and Reconnaissance
- Fingerprint Ports, Protocols, and Services
- Review Service Versions
- Enumerate Specific Application Stacks
- Identify Application Entry Points
- Map Execution Paths and Architecture

### P2P

- Sybil Attack
- Eclipse Attack
- Eavesdropping Attack

- Denial of Service Attack
- BGP Hijack Attack
- Alien Attack
- Timejacking

## **RPC**

- Eavesdropping Attack
- Denial of Service Attack
- The Ethereum Black Valentine's Day Vulnerability
- Http Input Attack
- Cross-Domain Phishing Attack

## **Consensus**

- Long Range Attack
- Bribery Attack
- Race Attack
- Liveness Denial
- Censorship
- Finney Attack
- Vector76 Attack
- Alternative Historical Attack
- 51% Attack
- Grinding Attack
- Coin Age Accumulation Attack
- Selfing Mining
- Block Double Production

## **Configuration and Deployment Management Testing**

- Test Network/Infrastructure Configuration
- Test Application Platform Configuration
- Test File Extensions Handling of Sensitive Information
- Identify API Exposure/Leakage
- Review Old, Backup, and Unreferenced Files for Sensitive Information
- Enumerate Infrastructure and Application Admin Interfaces

## **Authentication Testing**

- Test Default Credentials

- Test for Authentication Bypass
- Test for Valid User Enumeration

**Authorization Gathering**

- Test Directory Traversal/File Include
- Test for Bypassing Authorization Schema
- Test for Privilege Escalation
- Test for Insecure Direct Object References (IDORs)
- Test for Sensitive Data Leakage

**Data Validation Testing**

- Test for Server-Side Request Forgery (SSRF)
- Test for Remote Code Execution (RCE)
- Test for SQL Injection (Oracle, MySQL, SQL Server, PostgreSQL, MS Access, NoSQL)
- Test for LDAP Injection
- Test for XML Injection
- Test for IMAP/SMTP Injection
- Test for Code Injection (Local File Inclusion and Remote File Inclusion)
- Test for Command Injection
- Test for Buffer Overflow (Heap, Stack, Format string)
- Test for Incubated Vulnerabilities (i.e. Blind SQL Injection)

**Error Handling**

- Analyze Error Codes
- Analyze Stack Traces

**Cryptography**

- Test for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection
- Test for Sensitive Information Sent Via Unencrypted Channels

**Encryption**

- Cryptographic Attack
- Private Key Prediction
- Length Extension Attack
- Hash collision attack

- Transaction
- Transaction Replay Attack
- Transaction Malleability Attack
- Time-Locked Transaction Attack
- False Top-Up Attack
- Rug Pull Attack

## Audit Dashboard

Project	KleverChain
Auditors	Wesley Silva Luis Araujo
Assets	node.mainnet.klever.finance node.testnet.klever.finance
Networks	Node Mainnet /Node Testnet
Date	2021-06-30 to 2021-08-22

## Issues Found

	Low	Medium	High	Critical
Open	2	0	0	0
Resolved	1	0	0	0

## Results

Item	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Description	<p>The remote service has one of two configurations that are known to be required for the CRIME attack:</p> <ul style="list-style-type: none"> <li>• SSL / TLS compression is enabled.</li> <li>• TLS advertises the SPDY protocol earlier than version 4.</li> </ul> <p>Since this is an old version of the software, it may be vulnerable to attacks.</p>
Evidence	<pre> <b>TLS renegotiation:</b> Session renegotiation not supported  <b>TLS Compression:</b> Compression disabled  <b>Heartbleed:</b> TLSv1.3 not vulnerable to heartbleed TLSv1.2 not vulnerable to heartbleed  <b>Supported Server Cipher(s):</b> Preferred TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253 Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253 Accepted TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253 Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253 Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253 Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253 Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253 Accepted TLSv1.2 256 bits DHE-RSA-AES256-CCM8 DHE 2048 bits Accepted TLSv1.2 256 bits DHE-RSA-AES256-CCM DHE 2048 bits </pre> <p>The following configuration indicates that the remote service may be vulnerable to the CRIME attack :</p> <ul style="list-style-type: none"> <li>- SPDY support earlier than version 4 is advertised.</li> </ul>
Solution	Disable compression and/or the SPDY service.
Risk Factor	Low
Assets	Node.mainnet.klever.finance / node.testnet.klever.finance
Resolved	No. Very low probability to be exploited.



Item	IP Fragmentation Functionality 0 Length Fragment Handling Remote DoS
Description	<p>The remote host is prone to a denial of service attack. The remote host appears to be using a Linux kernel that contains a flaw in its IP fragment handling code.</p> <p>By sending a series of packets with 0-length fragments, an unauthenticated attacker may be able to disable the remote host's IP connectivity.</p>
Evidence	<pre> 17:30:21.759399 IP 1831/8255196.ctinets.com.38725 &gt; node.mainnet.klever.finance.21778: Flags [none], seq 0:12, win 31237, length 12 17:30:21.759404 IP ec2-34-235-69-194.eu-west-1.compute.amazonaws.com.13763 &gt; node.mainnet.klever.finance.11496: Flags [none], seq 0:12, win 14409, length 12 17:30:21.759410 IP node-1369.pool-188-180.dynamic.totinet.net.49568 &gt; node.mainnet.klever.finance.6797: Flags [none], seq 0:12, win 1147, length 12 17:30:21.759416 IP 230.238.53.190.58872 &gt; node.mainnet.klever.finance.33067: Flags [none], seq 0:12, win 27956, length 12 17:30:21.759421 IP c-67-177-250-103.hsd1.co.comcast.net.15193 &gt; node.mainnet.klever.finance.16429: Flags [none], seq 0:12, win 4894, length 12 17:30:21.759427 IP 26.119.79.3.17244 &gt; node.mainnet.klever.finance.56691: Flags [none], seq 0:12, win 8037, length 12 17:30:21.759432 IP 65.228.181.54.5951 &gt; node.mainnet.klever.finance.13724: Flags [none], seq 0:12, win 64015, length 12 17:30:21.759438 IP 112.64.242.132.7496 &gt; node.mainnet.klever.finance.10859: Flags [none], seq 0:12, win 46323, length 12 17:30:21.759461 IP server-108-138-40-81.waw51.r.cloudfront.net.33283 &gt; node.mainnet.klever.finance.7634: Flags [none], seq 0:12, win 56652, length 12 17:30:21.759467 IP 102.242.118.114.30828 &gt; node.mainnet.klever.finance.27259: Flags [none], seq 0:12, win 2247, length 12 17:30:21.759474 IP 142.187.4.37.46721 &gt; node.mainnet.klever.finance.37697: Flags [none], seq 0:12, win 27883, length 12 17:30:21.759480 IP ec2-13-113-43-76.ap-northeast-1.compute.amazonaws.com.19734 &gt; node.mainnet.klever.finance.50861: Flags [none], seq 0:12, win 18298, length 12 17:30:21.759486 IP 220.225.159.211.44251 &gt; node.mainnet.klever.finance.54859: Flags [none], seq 0:12, win 53439, length 12 17:30:21.759494 IP 10.143.252.211.31236 &gt; node.mainnet.klever.finance.30008: Flags [none], seq 0:12, win 39071, length 12 17:30:21.759502 IP 49.97.215.197.27208 &gt; node.mainnet.klever.finance.26251: Flags [none], seq 0:12, win 41448, length 12 17:30:21.759507 IP 38.199.129.34.21137 &gt; node.mainnet.klever.finance.32002: Flags [none], seq 0:12, win 6416, length 12 17:30:21.759514 IP 56.43.237.89.34842 &gt; node.mainnet.klever.finance.25163: Flags [none], seq 0:12, win 10466, length 12 17:30:21.759520 IP 210.227.255.220.7728 &gt; node.mainnet.klever.finance.47649: Flags [none], seq 0:12, win 5326, length 12 17:30:21.759528 IP 58.247.18.77.59973 &gt; node.mainnet.klever.finance.8701: Flags [none], seq 0:12, win 60443, length 12 17:30:21.759533 IP 160.202.3.108.53866 &gt; node.mainnet.klever.finance.24014: Flags [none], seq 0:12, win 35008, length 12 17:30:21.759541 IP 119.233.126.74.61165 &gt; node.mainnet.klever.finance.45182: Flags [none], seq 0:12, win 6479, length 12 17:30:21.759546 IP 87-40-147-181.ptr.edu.ie.41136 &gt; node.mainnet.klever.finance.54771: Flags [none], seq 0:12, win 39770, length 12 17:30:21.759554 IP 245.71.99.36.5582 &gt; node.mainnet.klever.finance.13177: Flags [none], seq 0:12, win 53152, length 12 17:30:21.759560 IP 249.43.184.99.38023 &gt; node.mainnet.klever.finance.49768: Flags [none], seq 0:12, win 40372, length 12 17:30:21.759567 IP 62.142.49.12.64911 &gt; node.mainnet.klever.finance.59777: Flags [none], seq 0:12, win 28654, length 12 17:30:21.759573 IP 47.245.120.115.58694 &gt; node.mainnet.klever.finance.45172: Flags [none], seq 0:12, win 12348, length 12 17:30:21.759580 IP 143.153.24.184.47330 &gt; node.mainnet.klever.finance.57012: Flags [none], seq 0:12, win 26428, length 12 17:30:21.759586 IP 99-35-228-20.lightspeed.brhml.sbcglobal.net.35748 &gt; node.mainnet.klever.finance.19186: Flags [none], seq 0:12, win 29578, length 12 17:30:21.759593 IP 40.100.69.231.49568 &gt; node.mainnet.klever.finance.34318: Flags [none], seq 0:12, win 9484, length 12 17:30:21.759599 IP 8.113.113.125.62104 &gt; node.mainnet.klever.finance.17035: Flags [none], seq 0:12, win 13720, length 12 17:30:21.759606 IP 77-164-186-89.fixed.kpn.net.58083 &gt; node.mainnet.klever.finance.42580: Flags [none], seq 0:12, win 61219, length 12 17:30:21.759612 IP 215.233.101.148.9631 &gt; node.mainnet.klever.finance.8248: Flags [none], seq 0:12, win 12612, length 12 17:30:21.759618 IP 28.164.171.97.44504 &gt; node.mainnet.klever.finance.26374: Flags [none], seq 0:12, win 24648, length 12 17:30:21.759625 IP 32.186.170.54.5704 &gt; node.mainnet.klever.finance.2459: Flags [none], seq 0:12, win 35568, length 12 17:30:21.759632 IP 99-188-176-219.lightspeed.mphntn.sbcglobal.net.16883 &gt; node.mainnet.klever.finance.13190: Flags [none], seq 0:12, win 41565, length 12 17:30:21.759638 IP static-del-59.176.159.3.bol.net.in.40260 &gt; node.mainnet.klever.finance.8637: Flags [none], seq 0:12, win 36792, length 12 17:30:21.759645 IP 189.149.128.137.5734 &gt; node.mainnet.klever.finance.33430: Flags [none], seq 0:12, win 59186, length 12 17:30:21.759652 IP 67.238.116.180.7021 &gt; node.mainnet.klever.finance.63130: Flags [none], seq 0:12, win 35526, length 12 17:30:21.759661 IP 230.82.88.216.45556 &gt; node.mainnet.klever.finance.17372: Flags [none], seq 0:12, win 6951, length 12 17:30:21.759666 IP dynamic-077-011-075-247.77.11.pool.telefonica.de.6151 &gt; node.mainnet.klever.finance.39400: Flags [none], seq 0:12, win 40801, length 12 17:30:21.759673 IP host-87-21-38-25.retail.telecomitalia.it.1171 &gt; node.mainnet.klever.finance.f5-globalsite: Flags [none], seq 0:12, win 59129, length 12 17:30:21.759679 IP 143.71.216.43.59263 &gt; node.mainnet.klever.finance.20281: Flags [none], seq 0:12, win 24680, length 12 17:30:21.759688 IP 37.36.190.9.32861 &gt; node.mainnet.klever.finance.47710: Flags [none], seq 0:12, win 63365, length 12 17:30:21.759693 IP 86.123.141.141.15785 &gt; node.mainnet.klever.finance.1514: Flags [none], seq 0:12, win 31779, length 12 17:30:21.759702 IP a126170032061.41.access-internet.ne.jp.21028 &gt; node.mainnet.klever.finance.10491: Flags [none], seq 0:12, win 4778, length 12 17:30:21.759707 IP 198.10.120.148.1932 &gt; node.mainnet.klever.finance.51822: Flags [none], seq 0:12, win 52511, length 12 17:30:21.759715 IP 212.69.172.249.43627 &gt; node.mainnet.klever.finance.32919: Flags [none], seq 0:12, win 3543, length 12 17:30:21.759720 IP 202-66-235-65.static.hk.net.34413 &gt; node.mainnet.klever.finance.58302: Flags [none], seq 0:12, win 1371, length 12 17:30:21.759728 IP 48.35.52.239.35973 &gt; node.mainnet.klever.finance.56429: Flags [none], seq 0:12, win 60315, length 12 17:30:21.759734 IP adsl-66-126-104-229.dsl.and02.pacbell.net.11298 &gt; node.mainnet.klever.finance.61043: Flags [none], seq 0:12, win 5226, length 12 17:30:21.759742 IP b2q-79-177-115-251.red.bzeqint.net.48258 &gt; node.mainnet.klever.finance.30996: Flags [none], seq 0:12, win 18021, length 12 17:30:21.759747 IP 11.108.163.1.3250 &gt; node.mainnet.klever.finance.34353: Flags [none], seq 0:12, win 46339, length 12 17:30:21.759756 IP 234.158.240.66.57322 &gt; node.mainnet.klever.finance.43125: Flags [none], seq 0:12, win 64255, length 12 17:30:21.759762 IP 202.196.57.244.13253 &gt; node.mainnet.klever.finance.54241: Flags [none], seq 0:12, win 18859, length 12 17:30:21.759769 IP 100.23.16.79.18994 &gt; node.mainnet.klever.finance.64325: Flags [none], seq 0:12, win 46739, length 12 17:30:21.759775 IP 62.184.7.110.30684 &gt; node.mainnet.klever.finance.57047: Flags [none], seq 0:12, win 23999, length 12 17:30:21.759782 IP 13.13.153.140.21988 &gt; node.mainnet.klever.finance.43803: Flags [none], seq 0:12, win 25840, length 12 17:30:21.759788 IP 157.187.6.78.43222 &gt; node.mainnet.klever.finance.58943: Flags [none], seq 0:12, win 51422, length 12 17:30:21.759796 IP 25-2-37-24.1410 &gt; node.mainnet.klever.finance.6823: Flags [none], seq 0:12, win 18219, length 12 </pre>
Solution	Effective protection only happens with a third-party solution. Example: Cloudflare.
Risk Factor	Low
Assets	Node.mainnet.klever.finance / node.testnet.klever.finance
Resolved	Yes. Configured DoS protection

## Conclusion

After using some tools and testing the environment described in this document, We have not found critical or high vulnerabilities.

All the security requirements have been archived during the architecture and coding phase.

## Appendix

### Severity

<b>Low</b>	<p>Low issues are generally subjective in nature or potentially deal with topics like "best practices" or "readability". Minor issues will in general not indicate an actual problem or bug in code.</p> <p>The maintainers should use their own judgment as to whether addressing these issues improves the codebase.</p>
<b>Medium</b>	<p>Medium issues are generally objective in nature but do not represent actual bugs or security problems. These issues should be addressed unless there is a clear reason not to.</p>
<b>High</b>	<p>High issues will be things like bugs or security vulnerabilities. These issues may not be directly exploitable or may require a certain condition to arise in order to be exploited.</p> <p>Left unaddressed, these issues are highly likely to cause problems with the operation of the contract or to lead to a situation that allows the system to be exploited in some way.</p>