SALUS SECURITY

May 2023

PENETRATION TESTING REPORT

NIBIRU

Overview

Project Name	Nibiru
File Name	Penetration Testing Report for Nibiru
Creator	Salus Security
Create Date	5 May 2023
Total days	5 Days
Receive Date	11 May 2023;25 May 2023

Modify History

Version	Modify Date	Modifier	Modify Type	Modified Chapter	Modified Content
2	25 May 2023	Nibiru	M		

*Modified Type are categorized by **A** - ADDED **M** - MODIFIED **D** – DELETED

Copyright Statement

Table of Contents

Introduction

1 About Salus Security

At Salus Security, we are in the business of trust. We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve. In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

2 Assessment Scope

Penetration testing coverage is assessed based on the scope of the asset that needs to be tested. Because the scope of this penetration test only includes assets under the main domain name of nibiru.fi. Therefore we have the high-level importance assets under the main domain name of nibiru.fi as the main assessment penetration object from the asset list. Therefore, This report reflects a detailed security summary report related to business security.

3 Risk Summary Description

Overall Risk Level: **Low**

Description: Through a security penetration test in a real environment, Nibiru was found to have dangerous vulnerabilities such as sensitive information leakage, certificate expiration. According to these vulnerabilities, it can be judged that they may be used by hackers or criminals, which will bear certain security risks.

4 Disclaimer

This report is considered by Salus Security to be private information; it is licensed to Nibiru under the terms of the project statement of work. Material within this report may not be reproduced or distributed in part or in whole without the express written permission of Salus Security.

Test Coverage Disclaimer
All activities undertaken by Salus Security in association with this project were performed in accordance with a statement of work and mutually agreed upon project plan. Security Penetration Testing projects are time-boxed and often reliant on the information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Salus Security uses automated testing techniques to test the controls and security properties of software rapidly. These techniques augment our penetration testing work, but each has its limitations. Their use is also limited by the time and resource constraints of a project.

Salus Security makes all effort but holds no responsibility for the findings of this penetration testing. Salus Security makes no judgments on the underlying business model or the individuals involved in the project.

5 Web Risk details

5.1 Weak Cipher Suites

Vulnerability Name:	Weak Cipher Suites
Risk Level:	Medium
Vulnerability Description:	TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.
Vulnerability Detail:	Use testssl to detect the corresponding domain name, and you can find that there are SSL related vulnerabilities.
Fix Suggestion:	Reconfigure the affected application to avoid use of weak cipher suites. Repair reference: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
Repair Status:	Acknowledge

5.2 Sensitive information disclosure

Vulnerability Name:	Sensitive information disclosure
Risk Level:	Medium
Vulnerability Description:	Sensitive information is leaked in the page or in the returned response package, which can be further infiltrated by an attacker.

Vulnerability Detail:	This page leaks a large number of Intranet IP addresses and node health monitoring status information.
Fix Suggestion:	Delete the page that is not related to services. If the page is a necessary middleware management page, you are advised to control the access permission of the page.
Repair Status:	Acknowledge

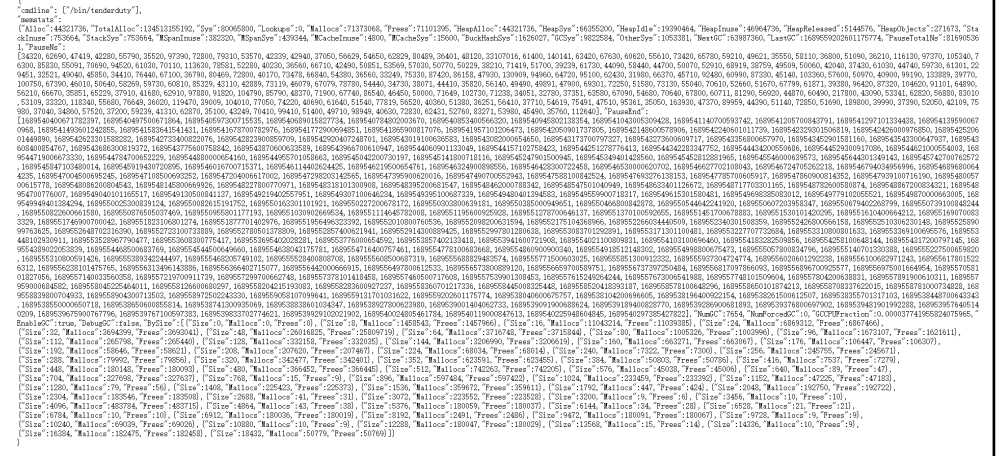
5.3 Varnish Unauthenticated Cache Purge

Vulnerability Name:	Varnish Unauthenticated Cache Purge
Risk Level:	Low
Vulnerability Description:	Cache Purge means to delete the stored caches. So if you purge the cache, it means the next time you visit that website, it will generate the page by pulling info from the database (the original method). Then, it will recopy the page again to create a new cache. If the Purge request is available to any user, even those who are not authenticated, they can delete/invalidate the caches stored at certain resource. This can lead to increased bandwidth costs and degraded application performance. Allowing anonymous users to purge cache could be used to maliciously degrade performance.

Vulnerability Detail:	If it is vulnerable it will look like this:
	Request
	`PURGE / HTTP/1.1`
	`Host: [redacted]`
	`User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2656.18 Safari/537.36`
	`Connection: close`
	`Accept: */*`
	`Accept-Language: en`
	`Accept-Encoding: gzip`
	Response
	`HTTP/1.1 200 OK`
	`Connection: close`
	`Content-Length: 50`
	`Accept-Ranges: bytes`
	`Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400`
	`Content-Type: application/json`
	`Date: Thu, 04 May 2023 10:53:09 GMT`
	`Fastly-Instant-Rate: 0`
	`Via: 1.1 varnish`
	`X-Served-By: cache-qpg1222-QPG`
	`X-Varnish: 2550360713`
	`{ "status": "ok", "id": "1222-1682697506-881443" }`

Fix Suggestion:	Disallow cache purge requests or limit to authenticated users only.
Repair Status:	Acknowledge

5.4 Golang Expvar information leaks

Vulnerability Name:	Golang Expvar information leaks
Risk Level:	Low
Vulnerability Description:	Exposes stack trace information and operation counters in the server,The debug page provided by the expvar variable. This page contains lots of critical live data about hardware and should not be available by default in production.
Vulnerability Detail:	
Fix Suggestion:	Hide or close the screen, and do not expose the screen to the Internet.
Repair Status:	Acknowledge

5.5 GraphQL Field Suggestion Information Disclosure

Vulnerability Name:	GraphQL Field Suggestion Information Disclosure
Risk Level:	Low
Vulnerability Description:	If introspection is disabled on your target, Field Suggestion can allow users to still earn information on the GraphQL schema. By default, GraphQL backends have a feature for fields and operations suggestions. If you try to query a field but you have made a typo, GraphQL will attempt to suggest fields that are similar to the initial attempt.

Vulnerability Detail:	Request:
	`POST /graphql HTTP/1.1`
	`Host: [redacted]`
	`User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.67 Safari/537.36`
	`Connection: close`
	`Content-Length: 69`
	`Content-Type: application/json`
	`Accept-Encoding: gzip`
	
	`{"query":"query {\n __schema {\n directive\n }\n}","variables":null}`
	
	Response:
	`HTTP/1.1 400 BAD REQUEST`
	`Connection: close`
	`Content-Length: 146`
	`Access-Control-Allow-Credentials: true`
	`Access-Control-Allow-Headers: DNT,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range,Authorization`
	`Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS`
	`Access-Control-Allow-Origin: *`
	`Access-Control-Max-Age: 1728000`
	`Content-Type: application/json`
	`Date: Sat, 06 May 2023 09:21:33 GMT`
	`Strict-Transport-Security: max-age=15724800; includeSubDomains`
	
	`{"errors":[{"message":"Cannot query field \"directive\" on type \"__Schema\". Did you mean \"directives\"?","locations":[{"line":3,"column":2}]}]}`

Fix Suggestion:	Repair reference: https://github.com/webonyx/graphql-php/issues/454
Repair Status:	Acknowledge

5.6 Cross-origin resource sharing

Vulnerability Name:	Cross-origin resource sharing
Risk Level:	Low
Vulnerability Description:	The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain. The application allowed access from the requested origin https://jzitakmwxcsa.com If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk. Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.
Vulnerability Detail:	Request:

	 Response: 
Fix Suggestion:	Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
Repair Status:	Acknowledge

5.7 TLS certificate expired

Vulnerability Name:	TLS certificate expired
Risk Level:	Low
Vulnerability Description:	TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed. It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS

	connections without user detection even when a valid TLS certificate is used.
Vulnerability Detail:	The following problem was identified with the server's TLS certificate: Certificate 3 in the certificate chain has expired. The server presented the following certificates: Server certificate Issued to: get.nibiru.fi Issued by: R3 Valid from: Sat May 06 00:01:27 CST 2023 Valid to: Fri Aug 04 00:01:26 CST 2023 Certificate chain #1 Issued to: R3 Issued by: ISRG Root X1 Valid from: Fri Sep 04 08:00:00 CST 2020 Valid to: Tue Sep 16 00:00:00 CST 2025 Certificate chain #2 Issued to: ISRG Root X1 Issued by: DST Root CA X3 Valid from: Thu Jan 21 03:14:03 CST 2021 Valid to: Tue Oct 01 02:14:03 CST 2024
Fix Suggestion:	Repair reference: https://wiki.mozilla.org/Security/Server_Side_TLS
Repair Status:	Acknowledge

Security Summary

Security Recommendations

1) Strictly control the access rights of relevant pages and check the rights of access roles.
2) Fuzzify relevant sensitive information, do it on the server side, and strictly check the data returned by the server side. the query data and page display data has to be consistent and never return redundant data.
3) Delete pages that are not related to the business. If it is a middleware management page that must be used, it is recommended to control the access rights of the page.