Web Front-end Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.11.10, the SlowMist security team received the TrendMicro team's security audit application for Chainsafer Web front-end, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of black box to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

Test method	Description
Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc.

The vulnerability severity level information:

Level	Description
Critical	Critical severity vulnerabilities will have a significant impact on the security of the project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the project in certain scenarios. It is suggested that the project team should evaluate and consider whether these vulnerabilities need to be fixed.
Weakness	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Suggestion	There are better practices for coding or architecture.

2 Audit Methodology

The security audit process of SlowMist security team for the application includes two steps:

- The codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.
- Manual audit of the codes for security issues. The application is manually analyzed to look for any potential issues.

The following is a list of security audit items considered during an audit:

NO.	Audit Items
1	HSTS security audit
2	X-Content-Type-Options security audit
3	X-XSS-Protection security audit
4	CSP security audit
5	HTTP cookies security audit
6	Web front-end storage security audit
7	Clickjacking protection security audit
8	XSS defense security audit
9	CSRF defense security audit
10	Third-party resource security audit
11	CORS security audit
12	postMessage security audit
13	Web API security audit
14	DNSSEC security audit
15	SSL/TLS security audit

NO.	Audit Items
16	Others

3 Project Overview

3.1 Project Introduction

Trend Micro ChainSafer provides advanced blockchain security with AI-powered algorithms that proactively detect and alert against suspicious activities. Leveraging Trend Micro's cybersecurity database, Trend Micro ChainSafer ensures your online transactions are safe and of the highest quality.

WebSite:

https://chainsafer.stag.nexone.io/snap/

3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

NO	Title	Category	Level	Status
N1	Lack of strict-transport-security response header	HSTS security audit	Low	Fixed
N2	Lack of X-Content-Type-Options response header	X-Content-Type-Options security audit	Low	Fixed
N3	Lack of X-XSS-Protection response header	X-XSS-Protection security audit	Low	Fixed
N4	Lack of Content-Security-Policy response header	CSP security audit	Low	Fixed
N5	Lack of X-Frame-Options response header	Clickjacking protection security audit	Low	Fixed

NO	Title	Category	Level	Status
N6	Lack of DNSSEC security configuration	DNSSEC security audit	Low	Fixed
N7	TLS protocol version enhancement	SSL/TLS security audit	Suggestion	Fixed

3.3 Vulnerability Summary

[N1] [Low] Lack of strict-transport-security response header

Category: HSTS security audit

Content

The website lacks of HSTS security response header, and can not ensure that all the data travels encrypted between the web browser and the server.

```
~: curl -s -v -D- https://chainsafer.stag.nexone.io/snap/ | grep -i "strict-transport-security:"

< HTTP/2 200
< content-type: text/html
< content-length: 1933
< date: Fri, 10 Nov 2023 02:30:05 GMT
< last-modified: Mon, 06 Nov 2023 08:57:54 GMT
< x-amz-server-side-encryption: AES256
< accept-ranges: bytes
< server: AmazonS3
< cache-control: public, max-age=0, s-maxage=2
< etag: "dc5c61925a069e728fbfd1524b01a994"
< vary: Accept-Encoding
< x-cache: Miss from cloudfront
< via: 1.1 200c95b73c59ce451775f143027d4164.cloudfront.net (CloudFront)
< x-amz-cf-pop: ATL58-P8
< x-amz-cf-id: BsdHhwbBScP_L5sJf3Yxd1kNdaobFODlc59uEmSx41yy82VKDfFNKw==
```

Solution

It is recommended to add a strict-transport-security response header to ensure that all the data travels encrypted between the web browser and the server.

For more information, please refer to: https://owasp.org/www-project-web-security-testing-guide/latest/4-

Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/07-Test_HTTP_Strict_Transport_Security

Status

Fixed

[N2] [Low] Lack of X-Content-Type-Options response header

Category: X-Content-Type-Options security audit

Content

The website lacks X-Content-Type-Options security response header and cannot avoid MIME type sniffing.

```
curl -s -v -D- https://chainsafer.stag.nexone.io/snap/ | grep -i "x-content-type-options:"

* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 200
< content-type: text/html
< content-length: 1933
< date: Fri, 10 Nov 2023 03:46:27 GMT
< last-modified: Mon, 06 Nov 2023 08:57:54 GMT
< x-amz-server-side-encryption: AES256
< accept-ranges: bytes
< server: AmazonS3
< cache-control: public, max-age=0, s-maxage=2
< etag: "dc5c61925a069e728fbfd1524b01a994"
< vary: Accept-Encoding
< x-cache: Miss from cloudfront
< via: 1.1 de692c0c5800b9c569f1a805c1518774.cloudfront.net (CloudFront)
< x-amz-cf-pop: ORD56-P4
< x-amz-cf-id: LQzh8yMZW0vV6AywAcXkCCf5cQo0UK9VXx0QNP4DRdxowLCa2wa7gA==
```

Solution

It is recommended to add x-content-type-options response header to avoid MIME type sniffing.

For more information, please refer to:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-content-type-options

Status

Fixed

[N3] [Low] Lack of X-XSS-Protection response header

Category: X-XSS-Protection security audit

Content

The website lacks X-XSS-Protection security response header and cannot block when the browser finds an XSS attack.

```
curl -s -v -D- https://chainsafer.stag.nexone.io/snap/ | grep -i "x-xss-protection:"

* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 200
< content-type: text/html
< content-length: 1933
< date: Fri, 10 Nov 2023 03:46:27 GMT
< last-modified: Mon, 06 Nov 2023 08:57:54 GMT
< x-amz-server-side-encryption: AES256
< accept-ranges: bytes
< server: AmazonS3
< cache-control: public, max-age=0, s-maxage=2
< etag: "dc5c61925a069e728fbfd1524b01a994"
< vary: Accept-Encoding
< x-cache: Miss from cloudfront
< via: 1.1 de692c0c5800b9c569f1a805c1518774.cloudfront.net (CloudFront)
< x-amz-cf-pop: ORD56-P4
< x-amz-cf-id: LQzh8yMZW0vV6AywAcXkCCf5cQo0UK9VXx0QNP4DRdxowLCa2wa7gA==
```

Solution

It is recommended to add X-XSS-Protection, which will block XSS when the browser detects an XXS attack.

For more information, please refer to:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-xss-protection

Status

Fixed

[N4] [Low] Lack of Content-Security-Policy response header

Category: CSP security audit

Content

The website lacks a Content-Security-Policy security response header and cannot restrict the reference of malicious resource data.

```
curl -s -v -D- https://chainsafer.stag.nexone.io/snap/ | grep -i "content-security-policy:"

* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 200
< content-type: text/html
< content-length: 1933
< date: Fri, 10 Nov 2023 03:46:27 GMT
< last-modified: Mon, 06 Nov 2023 08:57:54 GMT
< x-amz-server-side-encryption: AES256
< accept-ranges: bytes
< server: AmazonS3
< cache-control: public, max-age=0, s-maxage=2
< etag: "dc5c61925a069e728fbfd1524b01a994"
< vary: Accept-Encoding
< x-cache: Miss from cloudfront
< via: 1.1 de692c0c5800b9c569f1a805c1518774.cloudfront.net (CloudFront)
< x-amz-cf-pop: ORD56-P4
< x-amz-cf-id: LQzh8yMZW0vV6AywAcXkCCf5cQo0UK9VXx0QNP4DRdxowLCa2wa7gA==
```

Solution

It is recommended to add the Content-Security-Policy response header, which is only allowed to load resources from the specified source.

For more information, please refer to:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#content-security-policy-csp

Status

Fixed

[N5] [Low] Lack of X-Frame-Options response header

Category: Clickjacking protection security audit

Content

The website is missing the X-Frame-Options security header, which makes it vulnerable to clickjacking attacks.

```
curl -s -v -D- https://chainsafer.stag.nexone.io/snap/ | grep -i "x-frame-options:"

* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 200
< content-type: text/html
< content-length: 1933
< date: Fri, 10 Nov 2023 03:46:27 GMT
< last-modified: Mon, 06 Nov 2023 08:57:54 GMT
< x-amz-server-side-encryption: AES256
< accept-ranges: bytes
< server: AmazonS3
< cache-control: public, max-age=0, s-maxage=2
< etag: "dc5c61925a069e728fbfd1524b01a994"
< vary: Accept-Encoding
< x-cache: Miss from cloudfront
< via: 1.1 de692c0c5800b9c569f1a805c1518774.cloudfront.net (CloudFront)
< x-amz-cf-pop: ORD56-P4
< x-amz-cf-id: LQzh8yMZW0vV6AywAcXkCCf5cQo0UK9VXx0QNP4DRdxowLCa2wa7gA==
```

Solution

It is recommended to add x-frame-options to avoid click hijacking attacks.

For more information, please refer to:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-frame-options

Status

Fixed

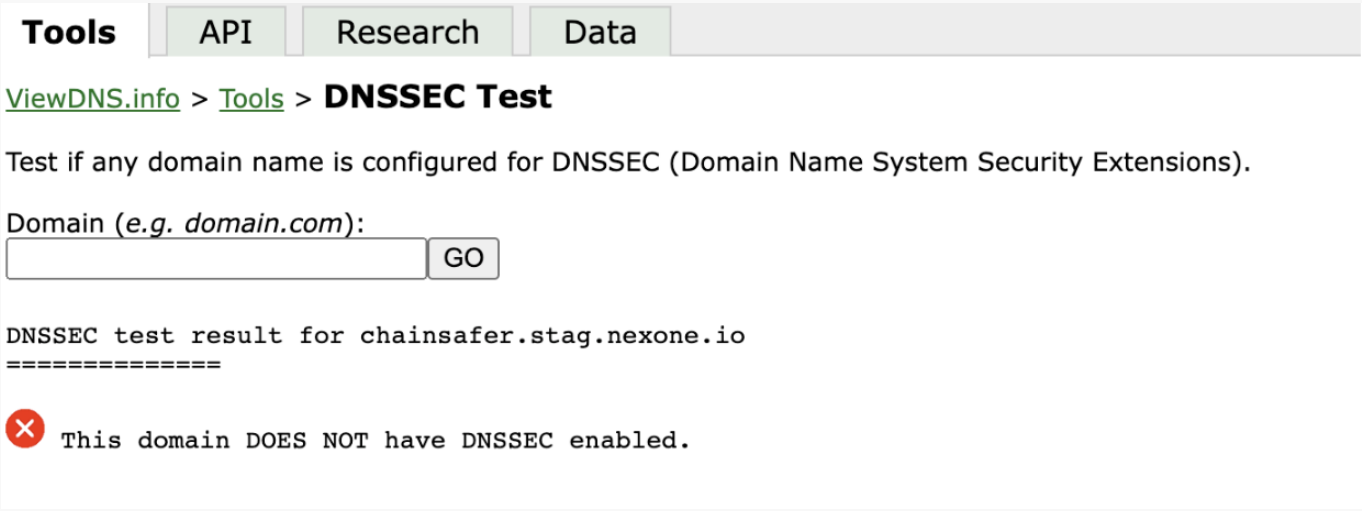
[N6] [Low] Lack of DNSSEC security configuration

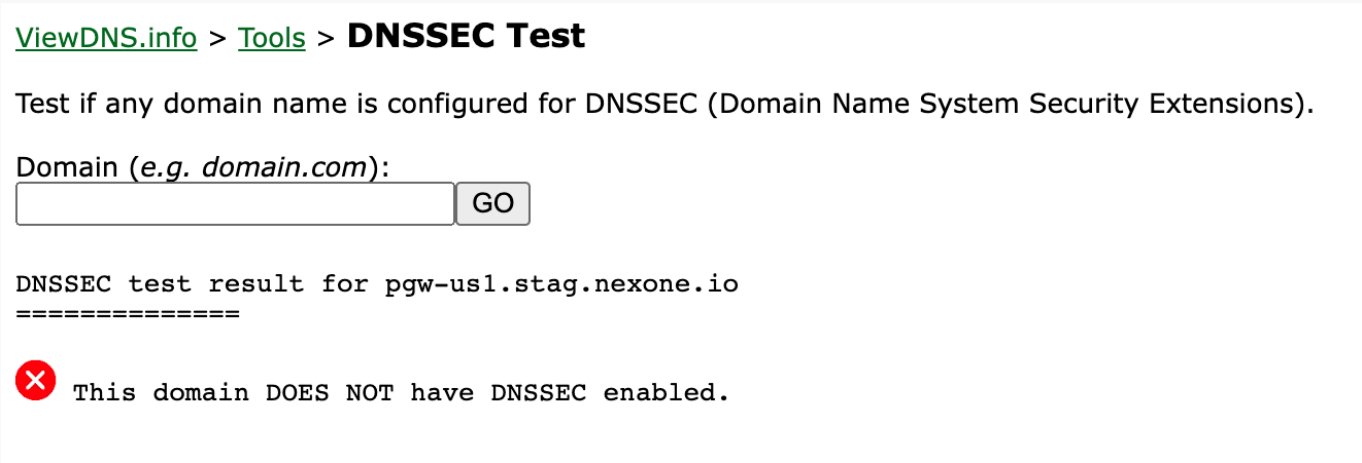
Category: DNSSEC security audit

Content

Lack of DNSSEC security configuration,Configuring DNSSEC can improve the security and reliability of websites or

applications.





Solution

It is recommended to enable DNS security in the domain name resolution service provider.

Status

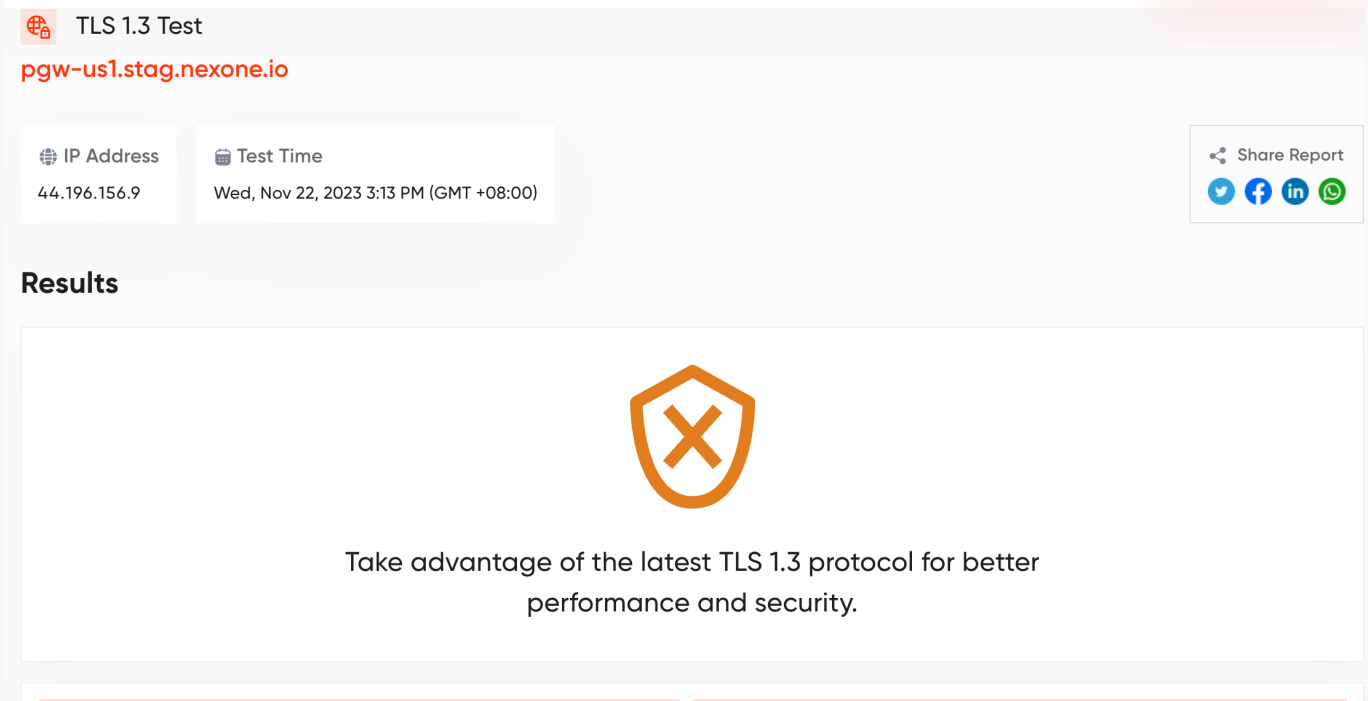
Fixed

[N7] [Suggestion] TLS protocol version enhancement

Category: SSL/TLS security audit

Content

The pgw-us1.stag.nexone.io does not support the latest TLS 1.3 protocol, but supports the older TLS 1.1 and TLS 1.0 protocols.



Solution

It is recommended to only support TLS 1.2 and TLS 1.3 protocols to improve security.

Status

Fixed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002311140002	SlowMist Security Team	2023.11.10 - 2023.11.14	Passed

Summary conclusion: The SlowMist security team uses a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 6 low-risk vulnerabilities and 1 suggestion. All findings have been fixed.

5 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist