CredShields

External Network Audit

Mar 4th, 2023 • CONFIDENTIAL

Description

This document details the process and result of the External Network audit performed by CredShields Technologies PTE. LTD. on behalf of Juno between Dec 12th, 2022, and Jan 12th, 2023. And a retest was performed on Feb 23rd, 2023.

Author

Shashank (Co-founder, CredShields)

shashank@CredShields.com

Reviewers

Aditya Dixit (Research Team Lead)

aditya@CredShields.com

Prepared for

Juno

Table of Contents

1. Executive Summary

Juno engaged CredShields to perform a External Network audit from Dec 12th, 2022, to Jan 12th, 2023. During this timeframe, Four (4) vulnerabilities were identified. **A retest was performed on Feb 23rd, 2023, and all the bugs have been addressed or acknowledged as won't fix.**

During the audit, Zero (0) vulnerabilities were found with a severity rating of either High or Critical. These vulnerabilities represent the greatest immediate risk to "Juno" and should be prioritized for remediation, and fortunately, none were found.

The table below shows the in-scope assets and a breakdown of findings by severity per asset. Section 2.3 contains more information on how severity is calculated.

Assets in Scope	Critical	High	Medium	Low	Info	Σ
External Network	0	0	0	4	0	**4**
	0	**0**	**0**	**4**	**0**	**4**

Table: Vulnerabilities Per Asset in Scope

The CredShields team conducted the security audit to focus on identifying vulnerabilities in External network scope during the testing window while abiding by the policies set forth by Juno's team.

State of Security

To maintain a robust security posture, it is essential to continuously review and improve upon current security processes. Utilizing CredShields' continuous audit feature allows both Juno's internal security and development teams to not only identify specific vulnerabilities but also gain a deeper understanding of the current security threat landscape.

To ensure that vulnerabilities are not introduced when new features are added, or code is refactored, we recommend conducting regular security assessments. Additionally, by analyzing the root cause of resolved vulnerabilities, the internal teams at Juno can implement both manual and automated procedures to eliminate entire classes of vulnerabilities in the future. By taking a proactive approach, Juno can future-proof its security posture and protect its assets.

2. Methodology

Juno engaged CredShields to perform a Juno External Network audit. The following sections cover how the engagement was put together and executed.

2.1 Preparation phase

The CredShields team performed a recon on all external network assets which were publicly facing the internet to look for vulnerabilities in it. They meticulously examined all functions and created a mind map to systematically identify potential security vulnerabilities, exposed networks, leaked data, and CVE detections.

A testing window from Dec 12th, 2022, to Jan 12th, 2023, was agreed upon during the preparation phase.

2.1.1 Scope

During the preparation phase, the following scope for the engagement was agreed-upon:

IN SCOPE ASSETS
***.juno.finance**

Table: List of Files in Scope

2.1.2 Documentation

Documentation was not required as the code was self-sufficient for understanding the project.

2.1.3 Audit Goals

CredShields uses both in-house tools and manual methods for comprehensive External Network audits. The majority of the audit is done by manually reviewing the publicly exposed network assets, following OWASP Web application security standards, and an extended industry standard self-developed checklist. The team places emphasis on understanding core concepts, preparing test cases, and evaluating business logic for potential vulnerabilities.

2.2 Retesting phase

Juno is actively partnering with CredShields to validate the remediations implemented towards the discovered vulnerabilities.

2.3 Vulnerability classification and severity

CredShields follows OWASP's Risk Rating Methodology to determine the risk associated with discovered vulnerabilities. This approach considers two factors - Likelihood and Impact - which are evaluated with three possible values - **Low**, **Medium**, and **High**, based on factors such as Threat agents, Vulnerability factors, Technical and Business Impacts. The overall severity of the risk is calculated by combining the likelihood and impact estimates.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Overall, the categories can be defined as described below -

1. **Informational**

   We prioritize technical excellence and pay attention to detail in our coding practices. Our guidelines, standards, and best practices help ensure software stability and reliability. Informational vulnerabilities are opportunities for improvement and do

not pose a direct risk to the organization. Code maintainers should use their own judgment on whether to address them.

2. **Low**

   Low-risk vulnerabilities are those that either have a small impact or can't be exploited repeatedly or those the client considers insignificant based on their specific business circumstances.

3. **Medium**

   Medium-severity vulnerabilities are those caused by weak or flawed logic in the code and can lead to exfiltration or modification of private user information. These vulnerabilities can harm the client's reputation under certain conditions and should be fixed within a specified timeframe.

4. **High**

   High-severity vulnerabilities pose a significant risk to the External Network and the organization. They can result in the loss of funds for some users, may or may not require specific conditions, and are more complex to exploit. These vulnerabilities can harm the client's reputation and should be fixed immediately.

5. **Critical**

   Critical issues are directly exploitable bugs or security vulnerabilities that do not require specific conditions. They often result in the loss of funds for users or put sensitive user information at risk of compromise or modification. The client's

reputation and financial stability will be severely impacted if these issues are not addressed immediately.

2.4 CredShields staff

The following individual at CredShields managed this engagement and produced this report:

- **Shashank, Co-founder CredShields**
    - shashank@CredShields.com

Please feel free to contact this individual with any questions or concerns you have around the engagement or this document.

3. Findings

This chapter contains the results of the security assessment. Findings are sorted by their severity and grouped by the asset and CWE classification. Each asset section will include a summary. The table in the executive summary contains the total number of identified security vulnerabilities per asset per risk indication.

3.1 Findings Overview

3.1.1 Vulnerability Summary

During the security assessment, Four (4) security vulnerabilities were identified in the asset.

VULNERABILITY TITLE	SEVERITY	CWE | Vulnerability Type
Plaintext Protocols	Low	Cleartext Transmission of Sensitive Information - CWE- 319
Outdated Nginx	Low	Components with Known Vulnerabilities - CWE-1104
Misconfigured SSL Certificates	Low	Improper Certificate Validation - CWE - 295
Plaintext Protocols	Low	Cleartext Transmission - CWE- 319

Table: Findings in External Network

4. Remediation Status

Juno is actively partnering with CredShields from this engagement to validate the discovered vulnerabilities' remediations. **A retest was performed on Feb 23rd, 2023, and all the issues have been addressed or acknowledged as won't fix.**

Also, the table shows the remediation status of each finding.

VULNERABILITY TITLE	SEVERITY	REMEDIATION STATUS
Plaintext Protocols	Low	**Fixed [23/02/2023]**
Outdated Nginx	Low	**Won't Fix**
Misconfigured SSL Certificates	Low	**Won't Fix**
Plaintext Protocols	Low	**Fixed [23/02/2023]**

Table: Summary of findings and status of remediation

5. Bug Reports

Bug ID#1 [Fixed]

TLS 1.0 and 1.1 Supported

Vulnerability Type
Inadequate Encryption Strength - CWE-326

Severity
Low

Description
Due to historic export restrictions of high-grade cryptography, legacy and new web servers are often able and configured to handle weak cryptographic options.
Even if high-grade ciphers are normally used and installed, some server misconfiguration could be used to force the use of a weaker cipher to gain access to the supposed secure communication channel.

In this case, the use of TLS 1.0 and TLS 1.1 were detected, which are almost deprecated (March 2020). As well as the use of a suite of weak ciphers in different versions of TLS was found.
A sophisticated attacker who's able to perform man-in-the-middle (MITM) attacks might be able to intercept and decrypt sensitive data due to a weak TLS configuration.

Vulnerable URL

- 44.224.133.234:443
- 52.42.120.33:443
- 54.183.1.55:8082

PoC

1. Scan the server using SSLLabs to view the results.

Impacts

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018.

Remediation

As a best practice, It is recommended to disable TLS1.0 and TLS1.1. Replace them with TLS 1.2 or higher. Consider supporting only cipher suites that are known to be secure.

Disable any cipher suites that use encryption with less than 128-bit key lengths or utilize RC4 algorithms. Enabled TLS cipher suites must be ranked as MEDIUM strength by the current version of OpenSSL at a minimum, however, HIGH is ideal. Ensure that the cipher suites are ordered from strongest to weakest.
Here's a reference - https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

Retest

This has been remediated.

Bug ID#2 [Won't Fix]

Outdated Nginx

Vulnerability Type
Components with Known Vulnerabilities - CWE-1104

Severity
Low

Description
The application was found to be using a vulnerable and outdated version of Nginx 1.10.3.

Vulnerable URLs

- 54.177.178.240:80
- 52.42.120.33:80
- 13.214.104.160:80
- 52.42.120.33:443
- 44.224.133.234:443
- https://nuo-defi-buybtc-web-prod-lb-744748610.ap-southeast-1.elb.amazonaws.com

PoC

1. The Nginx version can be seen in the response headers.

Impacts
Nginx 1.10.3 is affected by multiple vulnerabilities and publicly available exploits such as RCE, Denial of Service, etc.

References
https://www.cybersecurity-help.cz/vdb/nginx/nginx/1.10.3/

Remediation
Update the software to its latest version.

Retest

54.177.178.240:80 is not being used. All the others are non-production resources and therefore won't be fixed.

Bug ID#3 [Won't fix]

Misconfigured SSL Certificates

Vulnerability Type
Improper Certificate Validation - CWE - 295

Severity
Low

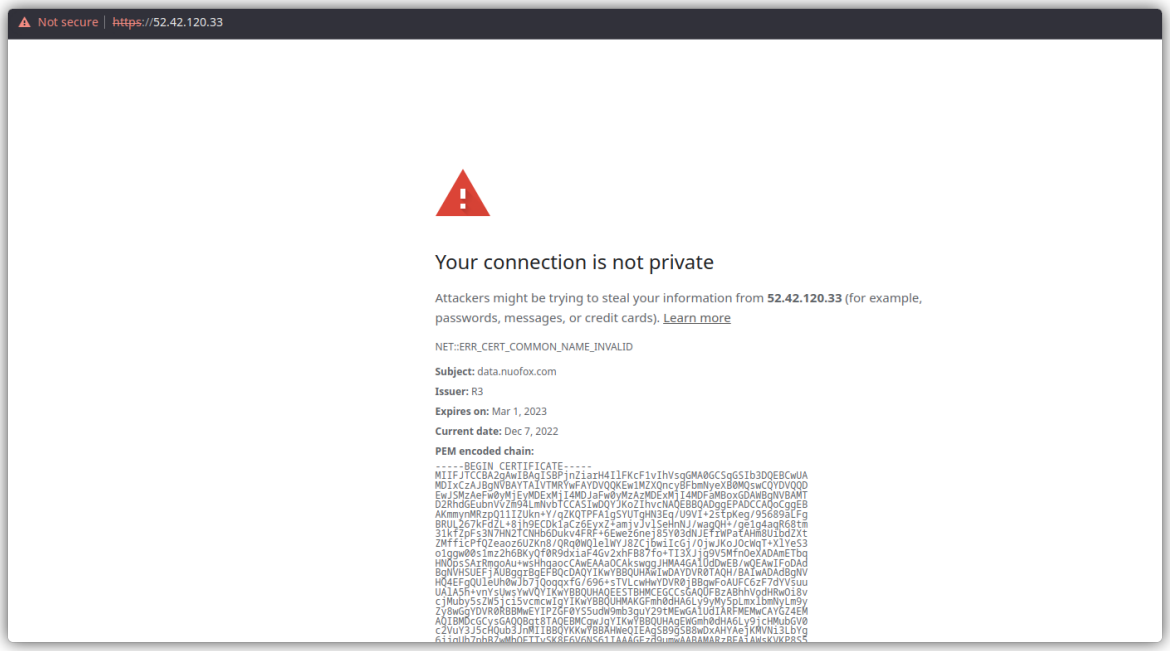
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that is not supported is recognized.

Vulnerable URLs
- 52.42.120.33:443
- 52.66.220.216:443
- 54.201.170.116:443
- 44.224.133.234:443
- 54.183.1.55:8082

PoC

1. The error can be seen in your browser or when you view the certificate details as shown below:



Impacts

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Remediation

Purchase or generate a proper SSL certificate for these services.

Retest

The assets are either non-production resources or not being used anymore, therefore won't be fixed.

Bug ID#4 [Fixed]

Plaintext Protocols

Vulnerability Type
Cleartext Transmission of Sensitive Information - CWE- 319

Severity
Low

Description
Various web servers serve content over TCP port 80, the cleartext HTTP protocol. This allows logins or data to be sent over unencrypted connections, which can allow a well-positioned attacker to capture user credentials or sensitive data by sniffing traffic.

Vulnerable URL

- http://13.214.104.160/
- http://35.87.246.115/
- http://54.177.178.240/
- http://54.201.170.116/

PoC

1. Browse any of the hosts listed above and observe that they accept HTTP traffic.

Impacts
This vulnerability might allow MitM attackers to compromise the data in transit.

Remediation
Do not support HTTP and redirect all traffic to HTTPS with proper implementation of the HSTS header.

Retest
This has been remediated. Resources are not being used and/or are unreachable externally**.**

6. Disclosure

The Reports provided by CredShields is not an endorsement or condemnation of any specific project or team and do not guarantee the security of any specific project. The contents of this report are not intended to be used to make decisions about buying or selling tokens, products, services, or any other assets and should not be interpreted as such.

Emerging technologies such as Web3 carry a high level of technical risk and uncertainty. CredShields does not provide any warranty or representation about the quality of code, the business model or the proprietors of any such business model, or the legal compliance of any business. The report is not intended to be used as investment advice and should not be relied upon as such.

CredShields Audit team is not responsible for any decisions or actions taken by any third party based on the report.