CredShields

AWS Security Audit

April 27th, 2023 • CONFIDENTIAL

Description

This document details the process and result of the AWS configuration audit performed by CredShields Technologies PTE. LTD. on behalf of Juno between Dec 3rd, 2022, and Jan 18th, 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

CRED SHiELDS

1. Executive Summary

Juno engaged CredShields to perform an AWS configuration audit from Dec 3rd, 2022, to Jan 18th, 2023. During this timeframe, Forty-two (42) vulnerabilities were identified. **A retest was performed on Feb 23rd, 2023, and all the bugs have been addressed.**

During the audit, Nine (9) 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
AWS configuration	1	8	8	24	1	**42**
	1	**8**	**8**	**24**	**1**	**42**

Table: Vulnerabilities Per Asset in Scope

The CredShields team conducted the security audit to focus on identifying vulnerabilities in AWS configuration's scope during the testing window while abiding by the policies set forth by AWS configuration'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 the configuration 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 configuration audit. The following sections cover how the engagement was put together and executed.

2.1 Preparation phase

The CredShields team meticulously reviewed all provided documents and comments in the smart-contract code to gain a thorough understanding of the contract's features and functionalities. They meticulously examined all services and created a mind map to systematically identify potential security vulnerabilities, prioritizing those that were more critical and business-sensitive for the updated configuration.

A testing window from Dec 3rd, 2022, to Jan 18th, 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 AWS

Table: List of Files in Scope

2.1.2 Documentation

Documentation was not required as the read-only API key was provided to the team directly.

2.1.3 Audit Goals

CredShields uses both in-house tools and manual methods for comprehensive smart contract security auditing. The majority of the audit is done by manually reviewing the AWS configuration, following AWS security standards, and an extended industry standard self-developed checklist.

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 the detail of AWS configuration. Our guidelines, standards, and best practices help ensure AWS's

stability and reliability. Informational vulnerabilities are opportunities for improvement and do not pose a direct risk to the organization.

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 configuration 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 organization. They can result in the loss of data 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 compromisation of the organization and 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 vulnerability 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, Forty-two (42) security vulnerabilities were identified in the asset.

VULNERABILITY TITLE	SEVERITY	SWC | Vulnerability Type
ACM Certificate with Transparency Logging Set to Disabled	Low	Insufficient Logging - CWE-778
Content Distribution with Clear-Text Origin TLS Policy	Low	Cleartext Transmission of Sensitive Information - CWE-319
CloudTrail Logs Not Encrypted with KMS Customer Master Keys (CMKs)	Medium	Cleartext Storage of Sensitive Information - CWE-312
CloudTrail Data Logging Configuration Not Covering All Resources	Low	Insufficient Logging - CWE-778
AWS Config Not Enabled	Low	Insufficient Logging - CWE-778

EBS Snapshot Not Encrypted	High	Cleartext Storage of Sensitive Information - CWE-312
EBS Volume Not Encrypted	High	Cleartext Storage of Sensitive Information - CWE-312
Security Group Opens All Ports to All	Low	Security Misconfiguration
Security Group Opens All Ports to All	Low	Security Misconfiguration
Security Group Opens PostgreSQL Port to All	Low	Security Misconfiguration
Security Group Opens SSH Port to All	Low	Security Misconfiguration
Default Security Groups in Use	Low	Security Misconfiguration
Unused Security Group	Low	Security Misconfiguration
Drop Invalid Header Fields Disabled	Medium	Missing Best Practices
Load Balancer Allowing Clear Text (HTTP) Communication	High	Cleartext Transmission of Sensitive Information - CWE-319
Lack of Deletion Protection	High	Missing Best Practices
Lack of ELBv2 Access Logs	Low	Cleartext Transmission of Sensitive Information - CWE-319
Credentials Unused for 90 Days or Greater Are Not Disabled	Informative	Security Misconfiguration

Cross-Account AssumeRole Policy Lacks External ID and MFA	Low	Security Misconfiguration
Inline role Policy Allows "iam:PassRole" For All Resources	Low	Security Misconfiguration
Lack of Key Rotation	Low	Security Misconfiguration
Password Security	High	Security Misconfiguration
Root Account Used Recently	Informational	Security Misconfiguration
Root Account without MFA	High	Security Misconfiguration
Users without MFA	High	Security Misconfiguration
User with Multiple API Keys	Low	Security Misconfiguration
Single AZ RDS Instance	Low	Missing Best Practices
KMS Customer Master Keys (CMKs) with Rotation Disabled	Low	Security Misconfiguration
RDS Instance publicly accessible	Medium	Security Misconfiguration
Instance Storage Not Encrypted	Medium	Cleartext Storage of Sensitive Information - CWE-312
Short Backup Retention Period	Low	Security Misconfiguration
Cluster Database Encryption Disabled	Medium	Cleartext Storage of Sensitive Information - CWE-312
Cluster Publicly Accessible	Low	Security Misconfiguration

Domain Transfer Not Lock	High	Security Misconfiguration
Bucket Access Logging Disabled	Low	Security Misconfiguration
Bucket Allowing Clear Text (HTTP) Communication	Medium	Security Misconfiguration
Bucket without Default Encryption Enabled	Medium	Security Misconfiguration
Bucket without MFA Delete	Medium	Security Misconfiguration
Bucket without Versioning	Low	Security Misconfiguration
Bucket world-listable	Critical	Security Misconfiguration
Subnet without a Flow Log	Low	Insufficient Logging - CWE-778

Table: Findings in Smart Contracts

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.**

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

VULNERABILITY TITLE	SEVERITY	REMEDIATION STATUS
ACM Certificate with Transparency Logging Set to Disabled	Low	**NA [23/02/2023]**
Content Distribution with Clear-Text Origin TLS Policy	Low	**Fixed [23/02/2023]**
CloudTrail Logs Not Encrypted with KMS Customer Master Keys (CMKs)	Medium	**Fixed [23/02/2023]**
CloudTrail Data Logging Configuration Not Covering All Resources	Low	**Fixed [23/02/2023]**
AWS Config Not Enabled	Low	**Fixed [23/02/2023]**
EBS Snapshot Not Encrypted	High	**Fixed [23/02/2023]**
EBS Volume Not Encrypted	High	**Fixed [23/02/2023]**
Security Group Opens All Ports to All	Low	**Fixed [23/02/2023]**

Security Group Opens All Ports to All	Low	**Won't Fix [23/02/2023]**
Security Group Opens PostgreSQL Port to All	Low	**Fixed [23/02/2023]**
Security Group Opens SSH Port to All	Low	**Fixed [23/02/2023]**
Default Security Groups in Use	Low	**Fixed [23/02/2023]**
Unused Security Group	Low	**Fixed [23/02/2023]**
Drop Invalid Header Fields Disabled	Medium	**Fixed [23/02/2023]**
Load Balancer Allowing Clear Text (HTTP) Communication	High	**Fixed [23/02/2023]**
Lack of Deletion Protection	High	**Fixed [23/02/2023]**
Lack of ELBv2 Access Logs	Low	**Fixed [23/02/2023]**
Credentials Unused for 90 Days or Greater Are Not Disabled	Informative	**Fixed [23/02/2023]**
Cross-Account AssumeRole Policy Lacks External ID and MFA	Low	**Fixed [23/02/2023]**
Inline role Policy Allows "iam:PassRole" For All Resources	Low	**Fixed [23/02/2023]**
Lack of Key Rotation	Low	**Won't Fix [23/02/2023]**

Password Security	High	**Fixed [23/02/2023]**
Root Account Used Recently	Informational	**Fixed [23/02/2023]**
Root Account without MFA	High	**Fixed [23/02/2023]**
Users without MFA	High	**Fixed [23/02/2023]**
User with Multiple API Keys	Low	**Won't Fix [23/02/2023]**
Single AZ RDS Instance	Low	**Won't Fix [23/02/2023]**
KMS Customer Master Keys (CMKs) with Rotation Disabled	Low	**Won't Fix [23/02/2023]**
RDS Instance publicly accessible	Medium	**Won't Fix [23/02/2023]**
Instance Storage Not Encrypted	Medium	**Fixed [23/02/2023]**
Short Backup Retention Period	Low	**Fixed [23/02/2023]**
Cluster Database Encryption Disabled	Medium	**Fixed [23/02/2023]**
Cluster Publicly Accessible	Low	**NA [23/02/2023]**
Domain Transfer Not Lock	High	**Fixed [23/02/2023]**

Bucket Access Logging Disabled	Low	**Fixed [23/02/2023]**
Bucket Allowing Clear Text (HTTP) Communication	Medium	**Fixed [23/02/2023]**
Bucket without Default Encryption Enabled	Medium	**Won't Fix [23/02/2023]**
Bucket without MFA Delete	Medium	**Won't Fix [23/02/2023]**
Bucket without Versioning	Low	**Fixed [23/02/2023]**
Bucket world-listable	Critical	**Fixed [23/02/2023]**
Subnet without a Flow Log	Low	**Fixed [23/02/2023]**

Table: Summary of findings and status of remediation

5. Bug Reports

Bug ID#1 [Can’t Fix]

ACM Certificate with Transparency Logging Set to Disabled

Type
Insufficient Logging - CWE-778

Severity
Low

Affected Service
ACM

Description
The ACM (Amazon Certificate Manager) is a service provided by Amazon Web Services (AWS) that allows users to easily create, manage, and deploy SSL/TLS certificates for their websites and applications. It allows users to secure their websites and ensure that their users' data is protected while being transmitted over the internet.

When the transparency logging is set to disabled for an ACM certificate, it means that the certificate will not be logged in the Certificate Transparency (CT) logs. CT logs are public logs that store the hashes of all SSL/TLS certificates issued by publicly trusted certificate authorities, and are used to help detect fraudulent certificates. This means that the certificate will not be publicly available for inspection and will not be subject to the same level of scrutiny as certificates that are logged in the CT logs.

It is important to note that disabling transparency logging for an ACM certificate does not make the certificate any less secure, but it may affect the level of trust that users have in the certificate. It is up to the certificate owner to determine whether or not to enable

transparency logging for their certificate, based on their specific security needs and requirements.

Vulnerable Assets

- kunal.clientvpn.com
- sourabh.clientvpn.com
- pavan.clientvpn.com
- rajeshray.clientvpn.com
- mukesh.clientvpn.com
- clientvpn.com
- shekhar.clientvpn.com
- pavan.clientvpn.com
- mukesh.clientvpn.com
- clientvpn.com

Has *Transparency Logging Preference: DISABLED*

Remediation

Transparency Logging should be enabled as a best practice.
https://aws.amazon.com/blogs/security/how-to-get-ready-for-certificate-transparency/

Retest

This can't be fixed. There's no option to enable Transparency Logging as these are imported certificates.

Bug ID#2 [Fixed]

Content Distribution with Clear-Text Origin TLS Policy

Type
Cleartext Transmission of Sensitive Information - CWE-319

Severity
Low

Affected Service
CloudFront

Description
When a content distribution network (CDN) is configured with a clear-text origin TLS policy, it means that the CDN will not encrypt the traffic between the origin server and the CDN edge servers. This means that any data sent from the origin server to the CDN edge servers will be transmitted in plain text, without being encrypted.

In some cases, the origin server may be located on a private network, and the traffic between the origin server and the CDN edge servers may be transmitted over a secure, private network connection. In these cases, the clear-text origin TLS policy may be appropriate, as the traffic is already being transmitted over a secure connection.

However, in other cases, the origin server may be located on the public internet, and the traffic between the origin server and the CDN edge servers may be transmitted over the public internet. In these cases, a clear-text origin TLS policy may not be appropriate, as the traffic is not being transmitted over a secure connection and could be intercepted by third parties. In these cases, it may be advisable to use a different TLS policy that encrypts the traffic between the origin server and the CDN edge servers.

Vulnerable Assets

- E3RI1ASSRHWQOK
  Has protocol policy set to *Protocol Policy: http-only*

Remediation

Distributing content between AWS CloudFront distributions and their custom origins over clear-text HTTP, without using AWS encryption solutions, can potentially expose sensitive data. Use secure connection instead.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-cloudfront-distribution-customoriginconfig.html

Retest

Bug ID#3 [Fixed]

CloudTrail Logs Not Encrypted with KMS Customer Master Keys (CMKs)

Type
Cleartext Storage of Sensitive Information - CWE-312

Severity
Medium

Affected Service
Cloudtrail

Description
By default, the log files delivered by CloudTrail to your bucket are encrypted with Amazon S3-managed encryption keys (SSE-S3). To get control over key rotation and obtain auditing visibility into key usage, use SSE-KMS to encrypt your log files with customer managed KMS keys.
Encrypting CloudTrail logs with KMS customer master keys allows users to have more control over the encryption keys used to protect their logs. This can provide an additional layer of security for the logs, as the keys are managed and controlled by the user, rather than by AWS.

Vulnerable Assets

-

Remediation
To have more control over the encryption and security of the log files, you can instead use server-side encryption with AWS KMS keys (SSE-KMS) for your CloudTrail log files.

Retest

Bug ID#4 [Fixed]

CloudTrail Data Logging Configuration Not Covering All Resources

Type
Insufficient Logging - CWE-778

Severity
Low

Affected Service
Cloudtrail

Description
In AWS, data logging can be configured using various services, such as CloudTrail, VPC Flow Logs, and CloudWatch Logs. These services allow users to collect and store data generated by various AWS resources, such as EC2 instances, S3 buckets, and Lambda functions.
However, it is important to ensure that the data logging configuration covers all resources in the system or application. This will ensure that all data is being collected and stored, and that the system or application can be monitored and managed effectively
CloudTrail Data Logging is not configured to cover all S3 or Lambda resources, which means that all S3 access and Lambda invocations are not logged.

Vulnerable Assets

- management-events
  The data event is set to Unknown *Data Events: Unknown*

Remediation
S3 bucket logging can be used in place of CloudTrail data events for S3. If that is the case, logs for Lambda invocations may still be missing.

Retest
As per the screenshot provided by the team, this has been resolved.

Bug ID#5 [Fixed]

AWS Config Not Enabled

Type
Insufficient Logging - CWE-778

Severity
Low

Affected Service
AWS Config

Description
If no AWS Config recorders are configured, it means that changes to the configuration of AWS resources are not being logged. This can hinder security analysis, resource change tracking, and compliance auditing, as important information about the configuration of the resources is not being collected and stored.

Vulnerable Assets

- ap-northeast-1
- ap-northeast-2
- ap-northeast-3
- ap-south-1
- ap-southeast-1
- ap-southeast-2
- ca-central-1
- eu-central-1
- eu-north-1
- eu-west-1
- eu-west-2
- eu-west-3
- sa-east-1
- us-east-1

- us-east-2

The above assets have *AWS Config Recorder enabled: false*

Remediation

Enable AWS Config in all regions, define the resources you want to record in each region and include global resources (IAM resources)
https://aws.amazon.com/blogs/mt/aws-config-best-practices/

Retest

Bug ID#6 [Fixed]

EBS Snapshot Not Encrypted

Type
Cleartext Storage of Sensitive Information - CWE-312

Severity
High

Affected Service
EC2

Description
Encrypting EBS snapshots ensures that the data on the snapshots is secure and cannot be accessed by unauthorized users.
AWS allows users to encrypt EBS snapshots using keys that are managed by AWS Key Management Service (KMS).
Encrypting EBS snapshots is important for protecting the data on the snapshots, and ensuring that it cannot be accessed by unauthorized users. It is a recommended security practice, and can help users meet their compliance and security requirements.

Vulnerable Assets
Below is the list of affected assets under each regions.
- ap-south-1
snap-07da1e6b56a3db922
snap-0bf5a1a84c9871b78
snap-0ee039d5f11da2825

- ap-southeast-1
snap-016af7ac751ee7986

us-east-2
snap-08248f0d0c8e5fec9

- us-west-1
juno-packer-AMI-ubuntu-20.04-1666702386-cis-hardened
juno-packer-AMI-ubuntu-20.04-1666959072-cis-hardened
juno_AMI_1655391000
juno-packer-AMI-ubuntu-20.04-1666798605-cis-hardened
juno-packer-AMI-ubuntu-20.04-1666942318-cis-hardened
juno_dev_AMI_1647429313
snap-0489603d7b24f46c3
snap-05424af4568442ccf
juno_dev_AMI_1645702138
juno_AMI_api1_1653917445
juno_AMI_1657557310
juno-packer-AMI-ubuntu-20.04-1667218882-cis-hardened
snap-069a9f52e5e072952
juno_dev_AMI_1647357988
juno_AMI_1652695767
snap-077cea20d8b3c97ca
juno_AMI_1655441879
snap-07d47746fe4e5ee25
juno - 1645466846
juno_AMI_1655389789
juno-packer-AMI-ubuntu-20.04-1666863137-cis-hardened
juno - 1645533282
juno_AMI_1652695171
juno_dev_AMI_1647433308
snap-0b93f1cebac39320a
snap-0bf49e5b2b69c596e
snap-0c18a21bf53731662
juno_AMI_1652696282
juno_AMI_1655447369
snap-0cd8b04be1113fe7c
snap-0d02d8a37c5fd99b4
onjuno-dev-Golden-AMI-Latest

juno-packer-AMI-ubuntu-20.04-1666716376-cis-hardened

- us-west-2
snap-009503ca30a65a8a1
snap-036ec3c4556bc76cf
snap-051f0867f63e012af
juno_AMI_1649323528
snap-05a0409605f64fe3e
juno_AMI_1649310327
snap-0819b74f329a3d1d3
snap-08f4c51331712263f
snap-093aa07ed3b5ae284
snap-0b7d1529a2240019d
juno_dev_AMI_1647359226
snap-0db9d9268ed4262df
snap-0e9395066911c54bf
snap-0f7dc07107ff6c6e4
snap-0f911c8168b6ea1d9

Remediation
It is recommended to encrypt EBS snapshots.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Retest
This has been fixed on production resources only.

Bug ID#7 [Fixed]

EBS Volume Not Encrypted

Type
Cleartext Storage of Sensitive Information - CWE-312

Severity
High

Affected Service
EC2

Description
Amazon Elastic Block Store (EBS) is a service provided by Amazon Web Services (AWS) that allows users to create and manage block storage volumes for use with Amazon Elastic Compute Cloud (EC2) instances. EBS volumes are used to store data for EC2 instances.
AWS EBS volume encryption refers to the process of encrypting EBS volumes to protect their data from unauthorized access.

Vulnerable Assets
Below is the list of affected assets under each region
- ap-south-1
vol-0fbe264c89a1d8dc6

- ap-southeast-1
vol-03147ee991b53540b
vol-0f4df02c0371b5a08

- us-west-1
vol-00983b6a0e44d1a9d
vol-03f2a548a445931a6
Appsmith
vol-08d8c442e99186867

vol-0b23d35aa33e86b92
vol-0c2ae54d55928fe60
Pre-dev Env

- us-west-2
vol-008b376cad34fb402
vol-014205cce41e168ff
vol-01e31d6bdbee3010e
vol-01ef9812d6916e921
vol-025de90c86f8554d1
vol-027e124df28914fe7
vol-028c45130b3a17571
vol-032fd8073513238fa
vol-037db81e488a42fbb
vol-04aebe358e67771e5
vol-04c4778e9a5e8aa71
vol-058e906263889806a
data-nuofox
vol-080fa28b21b42bbfb
vol-088124b35573db904
vol-0887aafccac4a087a
vol-0a4bb43f6b8c4f214
internal-nuofox
Appsmith Prod
vol-0b49b327aa8957d97
cred-nuofox
cms-nuofox
vol-0e165c5562e62d663
vol-0e7d47cdc5619eb47
vol-0ee779494df81e7eb
monitor-nuofox

Remediation

It is recommended to encrypt EBS volumes.

Retest
This has been fixed on production resources only.

Bug ID#8 [Fixed]

Security Group Opens All Ports to All

Type
Security Misconfiguration

Severity
Low

Affected Service
EC2

Description
It was detected that all ports in the security group are open, and any source IP address could send traffic to these ports, which creates a wider attack surface for resources assigned to it.

Vulnerable Assets
- launch-wizard-1
- all-open

Remediation
Open ports should be reduced to the minimum needed to correctly operate and, when possible, source address restrictions should be implemented.

Retest
This has been remediated on the above-mentioned resources.

Bug ID#9[Won't Fix]

Security Group Opens PostgreSQL Port to All

Type
Security Misconfiguration

Severity
Low

Affected Service
EC2

Description
The security group was found to be exposing the PostgreSQL port to all source addresses. Well-known ports are commonly probed by automated scanning tools, and could be an indicator of sensitive services exposed to Internet. If such services need to be exposed, a restriction on the source address could help to reduce the attack surface of the infrastructure.

Vulnerable Assets
- nuo-defi-buybtc-prod-rds-sg
- crm-nuofox-db-sg
- internal-nuofox-db-sg

Remediation
Open ports should be reduced to the minimum needed to correctly operate and, when possible, source address restrictions should be implemented.

Retest
Won't fix because these are non-production resources.

Bug ID#10 [Fixed]

Security Group Opens SSH Port to All

Type
Security Misconfiguration

Severity
Low

Affected Service
EC2

Description
The security group was found to be exposing the SSH port to all source addresses. Well-known ports are commonly probed by automated scanning tools, and could be an indicator of sensitive services exposed to Internet. If such services need to be exposed, a restriction on the source address could help to reduce the attack surface of the infrastructure.

Vulnerable Assets

- nuo-defi-buybtc-prod-rds-sg
- crm-nuofox-db-sg
- internal-nuofox-db-sg

Remediation
Open ports should be reduced to the minimum needed to correctly operate and, when possible, source address restrictions should be implemented.

Retest
This has been fixed. SSH is not open to all.

Bug ID#11 [Fixed]

Default Security Groups in Use

Type
Security Misconfiguration

Severity
Low

Affected Service
EC2

Description
Your AWS account automatically has a default security group for the default VPC in each Region. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group for the VPC.
The use of default security groups can indicate a lack of intentional enforcement of the principle of least privilege.

Vulnerable Assets
- default

Remediation
Ensure resources are not within default security groups. Instead, create a custom security group tailored to each resource needs.

Retest
This has been remediated.

Bug ID#12 [Fixed]

Unused Security Group

Type
Security Misconfiguration

Severity
Low

Affected Service
EC2

Description
Non-default security groups were defined which were unused and may not be required. This being the case, their existence in the configuration increases the risk that they may be inappropriately assigned. The unused security groups should be reviewed and removed if no longer required.

Vulnerable Assets
- launch-wizard-1
- onjuno-staging-redis-SG
- onjuno-staging-api-ALB_SG
- onjuno-staging-web-EC2-SG
- onjuno-staging-api-EC2_SG
- all-open
- retool SG
- vpnSG
- onjuno-dev-web-EC2-SG
- juno-dev-testing-sg
- onjuno-prod-web-EC2-SG
- nuofox-crm-sg
- launch-wizard-3
- launch-wizard-4

- OnJuno-ELB-SG
- launch-wizard-5

Remediation

It is recommended to go through the security groups and remove the ones that are not needed anymore.

Retest

All the unused security groups have been removed.

Bug ID#13 [Fixed]

Drop Invalid Header Fields Disabled

Type
Missing Best Practices

Severity
Medium

Affected Service
ELB

Description
ELB supports a feature called "Drop Invalid Header Fields" that can be used to mitigate the risk of request smuggling attacks. Request smuggling attacks are a type of web application security vulnerability that involves sending multiple requests to a web server, where some of the requests are hidden or modified in such a way that they are not processed by the server as intended.

By enabling the "Drop Invalid Header Fields" feature in ELB, users can prevent these types of attacks by automatically dropping any requests that contain invalid or maliciously crafted header fields.

Vulnerable Assets

- nuo-defi-buybtc-web-prod-lb
  We will notice *routing.http.drop_invalid_header_fields.enabled: false*

Remediation
It is recommended to set the field “routing.http.drop_invalid_header_fields.enabled” to true.

Retest

Bug ID#14 [Fixed]

Load Balancer Allowing Clear Text (HTTP) Communication

Type
Cleartext Transmission of Sensitive Information - CWE-319

Severity
High

Affected Service
ELB

Description
Use of a secure protocol (HTTPS or SSL) is best practice for encrypted communication. A load balancer without a listener using an encrypted protocol can be vulnerable to eavesdropping and man-in-the-middle attacks.

Vulnerable Assets

- nuo-defi-buybtc-web-prod-lb
- juno-web-dev-ALB
- juno-api-dev-ALB
- juno-web-prod-ALB
- juno-api-prod-ALB

Remediation
You can create a load balancer that uses the SSL/TLS protocol for encrypted connections (also known as SSL offload). This feature enables traffic encryption between your load balancer and the clients that initiate HTTPS sessions, and for connections between your load balancer and your EC2 instances.

Retest
The ELB has HTTP to HTTPS redirection

Bug ID#15 [Fixed]

Lack of Deletion Protection

Type
Missing Best Practices

Severity
High

Affected Service
ELB

Description
In AWS, users can enable deletion protection on ELB load balancers to prevent them from being accidentally deleted. When deletion protection is enabled, users cannot delete the load balancer using the AWS Management Console, AWS CLI, or API calls. This can help protect the load balancer and the applications and resources behind it from being accidentally deleted, which could cause downtime and other issues.

Vulnerable Assets

- nuo-defi-buybtc-web-prod-lb
  The asset has the settings *deletion_protection.enabled: false*

Remediation
It is recommended to enable deletion protection on the ELBs.

Retest

Bug ID#16 [Fixed]

Lack of ELBv2 Access Logs

Type
Cleartext Transmission of Sensitive Information - CWE-319

Severity
Low

Affected Service
ELB

Description
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and identify security issues.

Vulnerable Assets

- nuo-defi-buybtc-web-prod-lb
- juno-web-dev-ALB
- juno-api-dev-ALB
- juno-web-prod-ALB
- juno-api-prod-ALB

The above assets have settings *access_logs.s3.enabled: false*

Remediation
Enabling ELB access logs can provide valuable information and benefits for monitoring, debugging, and analyzing the performance and usage of ELB load balancers and the applications and resources behind them.

Retest

Bug ID#17 [Fixed]

Credentials Unused for 90 Days or Greater Are Not Disabled

Type
Security Misconfiguration

Severity
Informative

Affected Service
IAM

Description
Disabling or removing unnecessary credentials will reduce the window of opportunity for compromised accounts to be used.

Vulnerable Assets

- kiran
- frontend-dev-build-s3
- Kavin

Remediation
Ensure that all credentials (including passwords and access keys) have been used and changed in the last 90 days. If not, consider removing them.

Retest

Bug ID#18 [Fixed]

Cross-Account AssumeRole Policy Lacks External ID and MFA

Type
Security Misconfiguration

Severity
Low

Affected Service
IAM

Description
When authorizing cross-account role assumption, either an External ID or MFA should be required. If the role is intended for use by a service, an External ID can prevent "confused deputy" attacks. If the role is intended for use by an external user, then MFA will strengthen the authentication by requiring a second factor.

Vulnerable Assets

- cloudwatch_grafana

Remediation
It is recommended to use “ExternalId” for cross-account roles as a multifactor authentication mechanism.

Retest

Bug ID#19 [Fixed]

Inline role Policy Allows "iam:PassRole" For All Resources

Type
Security Misconfiguration

Severity
Low

Affected Service
IAM

Description
Using "*" for the resource field might grant permissions to more resources than necessary, potentially introducing privilege escalation scenarios.

Vulnerable Assets

- Inline Policy
  onjuno-api-prod-codepipeline-role
  onjuno-api-staging-codepipeline-role
  onjuno-api-dev-codepipeline-role

- Managed Policy
  AdministratorAccess

Remediation
It is not recommended to use a wildcard in resources section in the policy. Go through the policy and resources to grant access on per-need basis.

Retest
This has been fixed.

Bug ID#20 [Won't Fix]

Lack of Key Rotation

Type
Security Misconfiguration

Severity
Low

Affected Service
IAM

Description
In case of access key compromise, the lack of credential rotation increases the period during which an attacker has access to the AWS account.

Vulnerable Assets

- CSFLE-prod-kms
- frontend-dev-build-s3
- juno-config-files-s3-dev
- pavankumar
- juno-config-files-s3-prod
- Terraform_user
- cloudwatch_grafana
- CSFLE-dev-kms
- frontend-prod-build-s3

Remediation
Proper implementation of key rotation in AWS is important for improving the security of data, and reducing the risks associated with key compromise.

Retest

There is production dependency. This can’t be fixed.

Bug ID#21 [Fixed]

Password Security

Type
Security Misconfiguration

Severity
High

Affected Service
IAM

Description
Security best practices in password policy dictates several pointers that should be followed to increase the overall credential security. The following issues were identified:

- The password policy did not enforce a minimum of 14 characters.
- Password expiration is disabled. As a result, compromised credentials could be used by potential attackers for a indefinite amount of time.
- The password policy allowed password reuse.
- Password expiration is disabled, or expiration time is set to a too high value.

Vulnerable Assets
Current password Policy settings
Minimum password length: 1
Require at least one uppercase letter: false
Require at least one lowercase letter: false
Require at least one number: false
Require at least one non-alphanumeric character: false
Enable password expiration: false
Prevent password reuse: false

Remediation

- Ensure the password policy is configured to require a minimum length.

- Password should periodically be changed and there should be a proper expiration policy.
- Ensure the password policy is configured to prevent password reuse
- Enable password expiration and set the expiration period to 90 days or less

Retest

The password policies have been updated to:

- Minimum password length: 10
- Require at least one uppercase letter: true
- Require at least one lowercase letter: true
- Require at least one number: true
- Require at least one non-alphanumeric character: true
- Enable password expiration: true
- Password expiration period (in days): 90
- Prevent password reuse: true
- Number of passwords to remember: 2
- Allow users to change their own password: true

Bug ID#22 [Fixed]

Root Account Used Recently

Type
Security Misconfiguration

Severity
Informational

Affected Service
IAM

Description
The root account is the most privileged user in an account. As a best practice, the root account should only be used when required for root-only tasks.

Vulnerable Assets

- Root account
  Password Last Used: Thu Dec 01 2022 13:33:50 GMT+0530 (India Standard Time)

Remediation
Go through the audit logs to validate what changes were made using the root account. Ensure that the account is not used for daily activities and only used for critical tasks not possible with other privileged accouts.

Retest

Bug ID#23 [Fixed]

Root Account without MFA

Type
Security Misconfiguration

Severity
High

Affected Service
IAM

Description
The root account is the most privileged user in an account. MFA adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS website, they're prompted for their user name and password and for an authentication code from their AWS MFA device.

Vulnerable Assets

- Root account
  MFA Active: false

Remediation
Enable MFA for the root account. It is also recommended to use a hardware-based MFA for root account due to its sensitive nature.

Retest

Bug ID#24 [Fixed]

Users without MFA

Type
Security Misconfiguration

Severity
High

Affected Service
IAM

Description
All IAM users should have MFA. MFA adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS website, they're prompted for their user name and password and for an authentication code from their AWS MFA device.

Vulnerable Assets

- frontend-dev-build-s3
- mukesh.bhatia
- Kavin
- Permita
- kiran
- vinay.s
- Himanshu
- kaushik
- rajesh.ray
- test_user

Remediation
Enable MFA for all users in the AWS account

Retest

Bug ID#25 [Fixed]

User with Multiple API Keys

Type
Security Misconfiguration

Severity
Low

Affected Service
IAM

Description
The user was configured to have more than one active API keys associated with the account.

Vulnerable Assets

- Terraform_user

Remediation
Go through the account and configuration, if not needed, remove redundant and unused API keys.

Retest

Bug ID#26 [Won't Fix]

Single AZ RDS Instance

Type
Missing Best Practices

Severity
Low

Affected Service
RDS

Description
In case of failure, with a single-AZ deployment configuration, should an availability zone specific database failure occur, Amazon RDS can not automatically fail over to the standby availability zone.

Vulnerable Assets

- nuo-defi-buybtc-prod-rds
- passbolt-db-prod
- crm-nuofox-db
- internal-nuofox-db

Remediation
One possible remediation for this issue is to implement a multi-AZ deployment configuration for your RDS instances. This will allow RDS to automatically failover to a standby availability zone in case of a database failure in the primary availability zone.

Retest
This won't be fixed since they are non-production resources.

Bug ID#27 [Won't Fix]

KMS Customer Master Keys (CMKs) with Rotation Disabled

Type
Security Misconfiguration

Severity
Low

Affected Service
KMS

Description
Cryptographic best practices discourage extensive reuse of encryption keys. Consequently, Customer Master Keys (CMKs) should be rotated to prevent usage of compromised keys.

Note that AWS KMS supports optional automatic key rotation only for customer managed CMKs.

Vulnerable Assets

- us-east-1
  bd572532-05d8-4a2c-80b5-50eeba6c1e99
  f29b5896-dda4-4f49-9fd5-bc6f7c89ef26
- us-west-1
  2916a11c-e486-4931-971e-eeb5b922503c
  b15d45bc-8846-4c17-824e-35ccb4ab305d
  cfabd0d6-b976-4dfc-be89-85a2ff7267ec
- us-west-2
  aa64daa1-c6a6-497f-aac2-a775f66efa69
  d22f1ae1-1490-49c3-be66-75bbbb2b6c6c

Remediation

For every KMS Customer Master Keys (CMKs), ensure that the option to rotate keys every year is enabled.

Retest

There is production dependency. This can’t be fixed.

Bug ID#28 [Won't Fix]

RDS Instance publicly accessible

Type
Security Misconfiguration

Severity
Medium

Affected Service
RDS

Description
AWS RDS (Amazon Relational Database Service) instances are not publicly accessible by default. However, if an RDS instance has been improperly configured and made publicly accessible, it can be vulnerable to attacks from the internet.

Vulnerable Assets

- nuo-defi-buybtc-prod-rds
  Endpoint:
  nuo-defi-buybtc-prod-rds.cesinon7swjy.ap-southeast-1.rds.amazonaws.com:5432
  Publicly Accessible: Enabled

Remediation
Instances should not be publicly accessible as this risks exposing sensitive data. Consider restricting access to the RDS instances.

Retest
This won't be fixed since they are non-production resources.

Bug ID#29 [Won't Fix]

Instance Storage Not Encrypted

Type
Cleartext Storage of Sensitive Information - CWE-312

Severity
Medium

Affected Service
RDS

Description
Amazon RDS can encrypt your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots.

Vulnerable Assets

- nuo-defi-buybtc-prod-rds
- passbolt-db-prod
- internal-nuofox-db
  Encrypted Storage: Disabled

Remediation
It is recommended to enable encryption for data at rest for RDS instances.

Retest
This won't be fixed since they are non-production resources.

Bug ID#30 [Fixed]

Short Backup Retention Period

Type
Security Misconfiguration

Severity
Low

Affected Service
RDS

Description
The backup retention period is a period of time between 0 and 35 days for which you can perform a point-in-time restore. Setting the backup retention period to 0 disables automated backups. The backup retention period was found to be set as low as 7 days.

Vulnerable Assets

- nuo-defi-buybtc-prod-rds
- crm-nuofox-db
- internal-nuofox-db
  Backup Retention Period: 7 days

Remediation
It is recommended that the retention period is set to at least 30 days. Having a short retention period will impact how far back in time the database can be restored to, and may affect integrity and availability of data.

Retest

Bug ID#31 [Fixed]

Cluster Database Encryption Disabled

Type
Cleartext Storage of Sensitive Information - CWE-312

Severity
Medium

Affected Service
Redshift

Description
Amazon Redshift provides support for encrypting your data at rest by enabling encryption for your clusters. When you enable encryption for a cluster, data stored on the cluster's disks is encrypted using advanced encryption standard (AES) 256-bit encryption. This provides an additional layer of security for your data, protecting it from unauthorized access.

Vulnerable Assets

- juno-prod-redshift
  Encrypted: false

Remediation
It is recommended to enable encryption for Redshift clusters.

Retest
Resource does not exist anymore

Bug ID#32 [Fixed]

Cluster Publicly Accessible

Type
Security Misconfiguration

Severity
Low

Affected Service
Redshift

Description
Redshift clusters should never be public, as this increases the risk of exposing sensitive data. Public accessibility means that other AWS users can access your cluster and the data stored in it.

Vulnerable Assets

- juno-prod-redshift
  Publicly accessible: true

Remediation
If you do not want your Redshift clusters accessible from the Internet or outside your VPC, disable the Redshift Publicly Accessible option.

Retest
Resource does not exist anymore

Bug ID#33 [Can’t Fix]

Domain Transfer Not Lock

Type
Security Misconfiguration

Severity
High

Affected Service
Route53

Description
The domain registries for all generic TLDs and many geographic TLDs let you lock a domain to prevent someone from transferring the domain to another registrar without your permission.
A domain lock prevents someone from transferring your domain to another registrar without your permission. Your domain's TLD does not support this feature.

Vulnerable Assets

- juno.fi

Remediation
Enable domain transfer lock

Retest
Transfer lock isn't supported for .fi domains

Bug ID#34 [Partially Fixed]

Bucket Access Logging Disabled

Type
Security Misconfiguration

Severity
Low

Affected Service
S3

Description
Server access logging provides detailed records of the requests that are made to a bucket. Server access logs can assist you in security and access audits, help you learn about your customer base, and understand your Amazon S3 bill.
Access logging was found to be disabled for the buckets mentioned below.

Vulnerable Assets

- onjuno-dev-terraform
- juno-public-backup
- aws-cloudtrail-logs-us-east-1-events
- juno-fi-cdn
- juno-data-lake-dev
- onjuno-api-reports-bucket
- onjuno-dev-codepipeline
- onjuno-prod-codepipeline
- onjuno-staging-codepipeline
- juno-android-builds
- juno-api-alb-logs
- onjuno-dev-route53-backup-bucket
- aws-config-bucket-514448826598
- juno-config-files

- onjuno-prod-logs-backup
- juno-kibana-backup-dev

Remediation
Ensure that S3 buckets have Logging enabled

Retest
Logging has been enabled on all the buckets except aws-cloudtrail-logs-us-east-1-events, aws-config-bucket-514448826598, juno-aws-prod-logs, and nuo-defi-aws-logs.

Bug ID#37 [Partially Fixed]

Bucket Allowing Clear Text (HTTP) Communication

Type
Security Misconfiguration

Severity
Medium

Affected Service
S3

Description
S3 buckets should never be configured to allow clear text (HTTP) communication. Clear text communication means that data is transmitted over the network without encryption, making it vulnerable to interception and compromise.

Vulnerable Assets

- onjuno-dev-terraform
- juno-public-backup
- aws-cloudtrail-logs-us-east-1-events
- juno-fi-cdn
- juno-data-lake-dev
- onjuno-api-reports-bucket
- onjuno-dev-codepipeline
- onjuno-prod-codepipeline
- onjuno-staging-codepipeline
- juno-android-builds
- juno-api-alb-logs
- onjuno-dev-route53-backup-bucket
- aws-config-bucket-514448826598
- juno-config-files
- onjuno-prod-logs-backup

- juno-kibana-backup-dev

Remediation
To ensure that your S3 buckets are secure, you should always enable HTTPS communication. A policy that denies access when "aws:SecureTransport": "false" can be used.

Retest
This has only been fixed on public buckets except juno-fi-cdn.

Bug ID#38 [Fixed]

Bucket without Default Encryption Enabled

Type
Security Misconfiguration

Severity
Medium

Affected Service
S3

Description
Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. This will ensure data-at-rest is encrypted

Vulnerable Assets

- juno-public-backup
- juno-fi-cdn
- juno-data-lake-dev
- onjuno-api-reports-bucket
- juno-api-alb-logs
- juno-config-files

Remediation
Make sure default encryption is enabled for all the affected buckets.

Retest
This has been fixed. Encryption has been enabled for the buckets.

Bug ID#39 [Won't Fix]

Bucket without MFA Delete

Type
Security Misconfiguration

Severity
Medium

Affected Service
S3

Description
MFA Delete is a feature in Amazon S3 that allows users to protect objects in a bucket from accidental or unauthorized deletion. When MFA Delete is enabled for a bucket, users must provide a valid multi-factor authentication (MFA) code in order to delete objects from the bucket. This provides an additional layer of security, as it prevents unauthorized users from deleting objects without the MFA code.

Vulnerable Assets

- onjuno-dev-terraform
- juno-public-backup
- aws-cloudtrail-logs-us-east-1-events
- juno-fi-cdn
- juno-data-lake-dev
- onjuno-api-reports-bucket
- onjuno-dev-codepipeline
- onjuno-prod-codepipeline
- onjuno-staging-codepipeline
- juno-android-builds
- juno-api-alb-logs
- onjuno-dev-route53-backup-bucket
- aws-config-bucket-514448826598

- juno-config-files
- onjuno-prod-logs-backup
- juno-kibana-backup-dev

Remediation

Enable MFA delete to help protect objects from accidental or unauthorized deletion. It should be noted that MFA Delete can only be configured on buckets that have versioning enabled.

Retest

This is not required on listed buckets.

Bug ID#40 [Won't Fix]

Bucket without Versioning

Type
Security Misconfiguration

Severity
Low

Affected Service
S3

Description
Versioning is a means of keeping multiple variants of an object in the same bucket. With versioning, you can easily recover from both unintended user actions and application failures. The following buckets did not enable versioning:

Vulnerable Assets

- juno-public-backup
- aws-cloudtrail-logs-us-east-1-events
- juno-data-lake-dev
- onjuno-api-reports-bucket
- onjuno-dev-codepipeline
- onjuno-prod-codepipeline
- onjuno-staging-codepipeline
- juno-api-alb-logs
- onjuno-dev-route53-backup-bucket
- aws-config-bucket-514448826598
- onjuno-prod-logs-backup
- juno-kibana-backup-dev

Remediation
Go through the assets and enable versionsing for buckets handling business-critical data.

Retest

As per Juno, versioning is not required on the buckets mentioned above.

Bug ID#41 [Fixed]

Bucket world-listable

Type
Security Misconfiguration

Severity
Critical

Affected Service
S3

Description
An S3 bucket has been found that was accessible for AllUsers. If sensitive information is stored in this bucket, it could be at risk of being accessed by potential attackers.

Vulnerable Assets

- https://onjuno-api-reports-bucket.s3.amazonaws.com/

Remediation
Go through the assets and enable versionsing for buckets handling business-critical data.

Retest
Bucket's ACL have been properly implemented.

Bug ID#42 [Fixed]

Subnet without a Flow Log

Type
Insufficient Logging - CWE-778

Severity
Low

Affected Service
VPC

Description
VPC flow logs are a feature of Amazon VPC that allows you to capture information about the IP traffic going to and from your VPC network interfaces. This includes details such as the source and destination IP addresses, port numbers, and the number of bytes and packets transferred.
VPC flow logs can be useful for a variety of purposes, such as monitoring the traffic in your VPC, identifying security threats, and troubleshooting connectivity issues. You can configure VPC flow logs to capture traffic at the VPC level, the subnet level, or the network interface level.

Vulnerable Assets

- ap-northeast-1
    - vpc-2ed93f48
    - subnet-cae64582
    - subnet-d6e64cfd
    - subnet-d8809283

- ap-northeast-2
    - vpc-4775c92c
    - subnet-47df3018
    - subnet-c4168dbf

    - subnet-e88694a4
    - subnet-fc3c9297

- ap-northeast-3
    - vpc-02046b6b
    - subnet-9127fedc
    - subnet-ce120bb6
    - subnet-d513ecbc

- ap-south-1
    - vpc-16ec197d
    - subnet-0ec08042
    - subnet-c24a58aa
    - subnet-cf44ceb4

- ap-southeast-1
    - vpc-5300f735
    - subnet-1e2dba47
    - subnet-267bb36e
    - subnet-9ea972f8

- ap-southeast-2
    - vpc-e803198f
    - subnet-0a9ce152
    - subnet-a56a96ed
    - subnet-fbd1139d

- ca-central-1
    - vpc-04b6976c
    - subnet-4b277123
    - subnet-693cd036
    - subnet-7a9af900

- eu-central-1

    - vpc-6c45fa06
    - subnet-67f62b1b
    - subnet-d17610bb
    - subnet-f970d0b5

- eu-north-1
    - vpc-927ac7fb
    - subnet-3bde0340
    - subnet-4348b40e
    - subnet-4aeb5923

- eu-west-1
    - vpc-01bf6878
    - subnet-8a2d3dc2
    - subnet-9e6123c4
    - subnet-c89697ae

- eu-west-2
    - vpc-69164a01
    - subnet-056ddc49
    - subnet-7a486e13
    - subnet-9f2341e5

- eu-west-3
    - vpc-4baa5f23
    - subnet-6b372702
    - subnet-86661acb
    - subnet-cbe7ccb0

- sa-east-1
    - vpc-d8b854be
    - subnet-36187c6d
    - subnet-430e920a
    - subnet-921d83f4

- us-east-1
    - vpc-7e954803
    - subnet-07b73558
    - subnet-2495c469
    - subnet-5065e971
    - subnet-71518440
    - subnet-95e869f3
    - subnet-fa5823f4

- us-east-2
    - onjuno-staging-vpc
    - onjuno-staging-public-subnets-3
    - onjuno-staging-public-subnets-2
    - onjuno-staging-public-subnets-1
    - vpc-6368d408
    - subnet-0152174d
    - subnet-b2aab8c8
    - subnet-e25bff89

- us-west-1
    - onjuno-dev-vpc
    - onjuno-dev-private-subnets-test
    - onjuno-dev-private-subnets-2
    - onjuno-dev-private-subnets-1
    - onjuno-dev-public-subnets-1
    - onjuno-dev-public-subnets-2
    - vpc-5127eb37
    - subnet-2d0bb44b
    - subnet-6648833c

- us-west-2
    - onjuno-prod-vpc
    - onjuno-prod-public-subnets-1

- onjuno-prod-private-subnets-2
- onjuno-prod-private-subnets-4
- onjuno-prod-private-subnets-1
- onjuno-prod-public-subnets-2
- onjuno-prod-public-subnets-4
- onjuno-prod-public-subnets-3
- onjuno-prod-private-subnets-3
- vpc-448bdc3c
- subnet-06874a4c
- subnet-1d903065
- subnet-206d470b
- subnet-412d9e1c

Remediation
Create a flow log for each subnet.

Retest
This has been fixed.

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 Smart Contracts and Solidity 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.