// HALBORN

Moonwell

Cloud Security Assessment

Prepared by: **Halborn**

Date of Engagement: **June 3rd, 2022 - Jun 8th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	06/08/2022	Bryan Recinos
0.2	Draft Review	06/09/2022	Alex Yang
1.0	Remediation Plan	07/20/2022	Bryan Recinos
1.1	Remediation Plan Review	07/21/2022	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Alex Yang	Halborn	Alex.Yang@halborn.com
Bryan Recinos	Halborn	Bryan.Recinos@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

Moonwell engaged Halborn to conduct a vulnerability scan on their Amazon Cloud infrastructure. The security assessment was scoped to all the services internally accessible with the given access level.

The outcome of this security audit has to be used as a reference for the system administration team to address the issues found on the cloud infrastructure scan.

The recommendations for the findings are listed at the end of each section of the report. Furthermore, an external custom Scout scan will be shared with the team and referenced on this report.

Halborn recommends performing further analysis to validate extended safety and remediation in context of the entire infrastructure when troubleshooting and adding new features.

1.2 AUDIT SUMMARY

The Halborn team was provided a timeline for the engagement to scan for vulnerabilities in internal cloud services, the goal of which is to accomplish the following:

- Find vulnerable services.
- Ensure that the exposed services are as intended and that sensitive data cannot be leaked.

It is highly recommended addressing the issues found to ensure the security of the infrastructure as far as possible.

1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of the cloud infrastructure pentest. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of the infrastructure and can quickly identify flaws in it. The following phases and associated tools were used throughout the term of the audit:

- Research into the infrastructure and the different services exposed.
- Automated service and instance scanning, enumeration and metadata extraction.
- Manually scan and validate the exposed services to confirm that automated scans are not false positives.
- Manually check each of the infrastructure services for not found issues during automated scans.
- Manually testing all the exposed services for security issues that could cause logical errors or data leakage on the platform.

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.
3 - Potential of a security incident in the long term.

2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

10 - CRITICAL
9 - 8 - HIGH
7 - 6 - MEDIUM
5 - 4 - LOW
3 - 1 - VERY LOW AND INFORMATIONAL

1.4 SCOPE

Halborn was given ReadOnly access to their AWS environments, facilitated by the HalbornCloudAudit cross-account role. Scans covered (among others) the following services:

Listing 1

```
ACM
CloudFormation
CloudTrail
CloudWatch
Config
EC2
IAM
KMS
RDS
SQS
S3
VPC
```

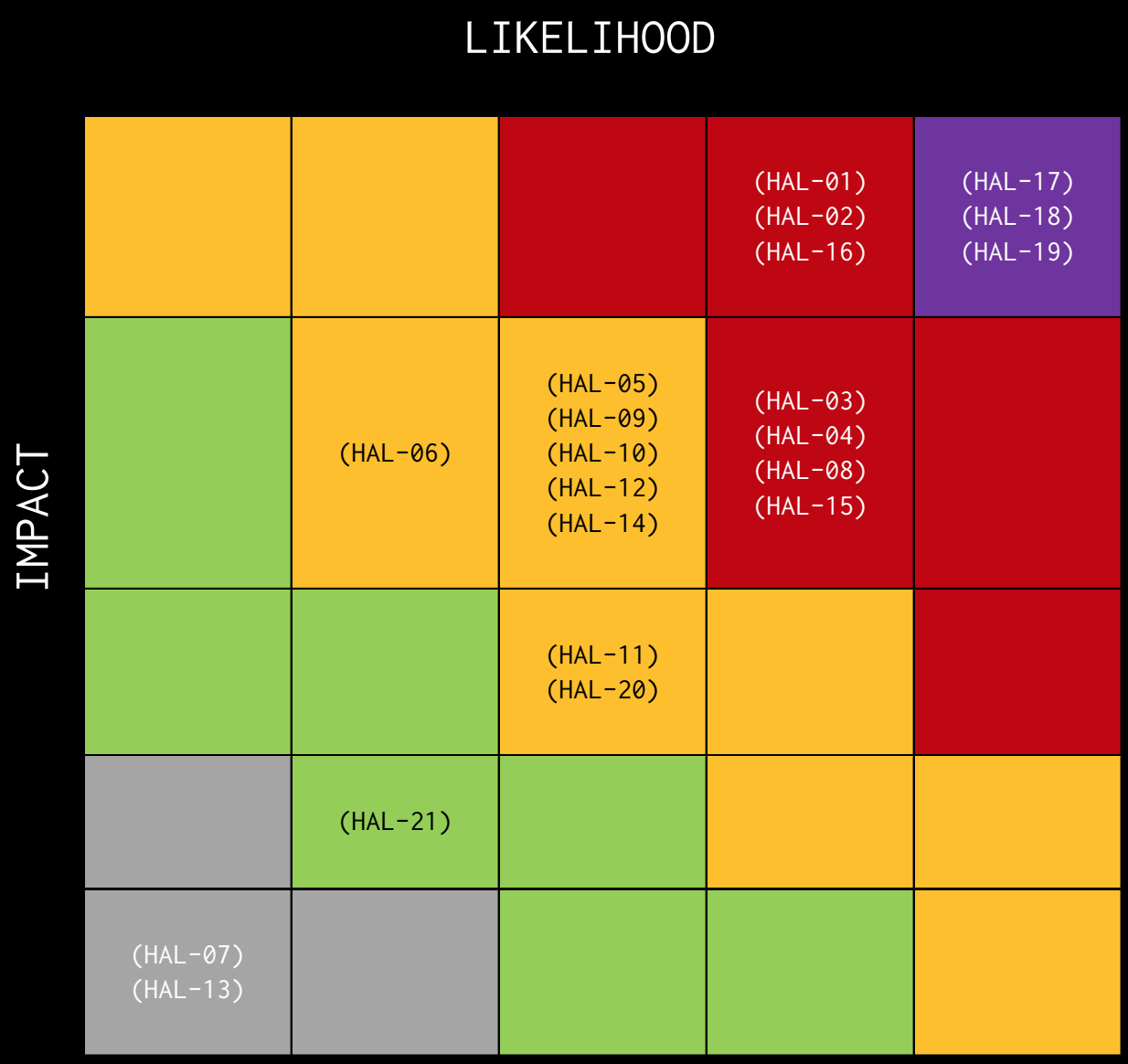
AWS Accounts audited:

- moonbeam: 054150576743
- moonriver: 615885558947
- moonwell-iam: 409295697534
- moonwell-dev: 234066291263
- moonwell-master: 348453866784

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
3	7	8	1	2

EXECUTIVE OVERVIEW



EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
(HAL01) - ARCHITECTURE - MISSING SCP POLICIES TO BLOCK UNUSED REGIONS	High	RISK ACCEPTED
(HAL02) - ARCHITECTURE - MISSING SCP POLICY TO DENY THE ABILITY TO LEAVE ORGANIZATION	High	SOLVED - 07/19/2022
(HAL03) - ARCHITECTURE - SINGLE AZ RDS INSTANCE	High	RISK ACCEPTED
(HAL04) - AUDIT AND LOGGING - AWS SECURITY HUB IS DISABLED	High	SOLVED - 07/19/2022
(HAL05) - AUDIT AND LOGGING - CLOUDTRAIL SERVICE NOT CONFIGURED	Medium	SOLVED - 07/19/2022
(HAL06) - AUDIT AND LOGGING - AWS CONFIG NOT ENABLED	Medium	SOLVED - 07/19/2022
(HAL07) - AUDIT AND LOGGING -LACK OF ELBV2 ACCESS LOGS	Informational	SOLVED - 07/19/2022
(HAL08) - DATA PROTECTION AND ENCRYPTION - LOAD BALANCER ALLOWING CLEAR TEXT (HTTP) COMMUNICATION	High	SOLVED - 07/19/2022
(HAL09) - DATA PROTECTION AND ENCRYPTION - EBS VOLUMES NOT ENCRYPTED	Medium	SOLVED - 07/19/2022
(HAL10) - DATA PROTECTION AND ENCRYPTION - EBS SNAPSHOT NOT ENCRYPTED	Medium	SOLVED - 07/19/2022
(HAL11) - DATA PROTECTION AND ENCRYPTION - LACK OF DELETION PROTECTION	Medium	SOLVED - 07/19/2022
(HAL12) - DATA PROTECTION AND ENCRYPTION - EBS DEFAULT ENCRYPTION DISABLED	Medium	SOLVED - 07/19/2022
(HAL13) - DATA PROTECTION AND ENCRYPTION - CONFIGURE AN AWS BACKUP PLAN	Informational	SOLVED - 07/19/2022
(HAL14) - DETECTION AND MONITORING - SCAN ON PUSH DISABLED ON ECR	Medium	SOLVED - 07/19/2022

(HAL15) - IAM - WEAK PASSWORD POLICY	High	PARTIALLY SOLVED - 07/19/2022
(HAL16) - IAM - ROOT ACCOUNT USED RECENTLY	High	SOLVED - 07/19/2022
(HAL17) - NETWORK SECURITY - DEFAULT VPC BEING USED	Critical	RISK ACCEPTED
(HAL18) - NETWORK SECURITY - SECURITY GROUP OPENS SSH PORT TO ALL	Critical	SOLVED - 07/19/2022
(HAL19) - NETWORK SECURITY - RDS PUBLICLY ACCESSIBLE ENABLED	Critical	SOLVED - 07/19/2022
(HAL20) - NETWORK SECURITY - DROP INVALID HEADER FIELDS DISABLED	Medium	SOLVED - 07/19/2022
(HAL21) - NETWORK SECURITY - UNUSED SECURITY GROUPS	Low	SOLVED - 07/19/2022

FINDINGS & TECH DETAILS

3.1 (HAL-01) ARCHITECTURE - MISSING SCP POLICIES TO BLOCK UNUSED REGIONS - HIGH

Description:

If your AWS account gets compromised, one of the most common attacks are based on launching really big and expensive EC2 instances and start mining on regions that you usually do not use; therefore it gets really hard to detect if you have EC2 instances running on those regions.

Recommendation:

It is recommended enabling AWS Organizations and create an SCP policy to block the creation of resources on regions that you don't use.

References:
Service control policies (SCPs)
Deny access to AWS based on the requested AWS Region

Remediation Plan:

RISK ACCEPTED: There are good practices in place to secure/vault root credentials and require 2FA and STS/assume role for all users. The risk of an account compromise is low for us and even if an account were to be compromised, EC2 limits would prevent very many instances from being launched. AWS typically refunds these incidents even if it does occur. The likelihood is also high that the Moonwell team might want to use other regions in the future, so the downsides to having to manage a policy outweigh the gain.

3.2 (HAL-02) ARCHITECTURE - MISSING SCP POLICY TO DENY THE ABILITY TO LEAVE ORGANIZATION - HIGH

Description:

Even though you set up multiple service control policies (SCPs) to enhance the security on your organization, member accounts still can leave the organization and the SCPs would no longer have effect on the member account.

Recommendation:

We recommend creating an SCP policy that prevent member accounts from leaving the organization.

Listing 2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

References:

Service control policies (SCPs)

Prevent member accounts from leaving the organization

Remediation Plan:

SOLVED: SCP has been created.

3.3 (HAL-03) ARCHITECTURE - SINGLE AZ RDS INSTANCE - HIGH

Description:

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

Affected Resources:

- arn:aws:rds:us-east-2:234066291263:db:moonbase-collector-db

Recommendation:

It is recommended to enable multi-az for RDS with critical application workloads.

References:
- Amazon RDS Multi-AZ

Remediation Plan:

RISK ACCEPTED: This is a development/testing database, and does not require the same level of high availability as the Moonwell production databases require. Therefore, it is only a single instance, which is standard for most of our dev/test (non-production) systems. All the Moonwell production RDS database instances have high availability enabled.

3.4 (HAL-04) AUDIT AND LOGGING - AWS SECURITY HUB IS DISABLED - HIGH

Description:

AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.

Affected accounts:

- 615885558947
- 409295697534
- 348453866784
- 234066291263
- 054150576743

Recommendation:

Recommend to enable AWS security hub on the regions you want to protect.

References:
Setting up AWS Security Hub
AWS Security Hub Pricing

Remediation Plan:

SOLVED: Security hub has been enabled.

3.5 (HAL-05) AUDIT AND LOGGING - CLOUDTRAIL SERVICE NOT CONFIGURED - MEDIUM

Description:

Cloudtrail service is not enabled, you can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

Affected Accounts:

- 054150576743
- 234066291263
- 348453866784
- 409295697534
- 615885558947

Recommendation:

It is recommended to enable cloudtrail on all the regions where your workloads are running, while enabling cloudtrail make sure that your logs are encrypted with a Customer Master Key (CMK).

References:
Creating a Trail for all regions
Creating a trail for an Organization

Remediation Plan:

SOLVED: Cloudtrail has been enabled.

3.6 (HAL-06) AUDIT AND LOGGING - AWS CONFIG NOT ENABLED - MEDIUM

Description:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

In case that someone performs a configuration change on a critical resource, AWS Config keeps track of each change perform on your resources, helping you to go back to a previous state of your resource.

Affected accounts:

- 615885558947
- 409295697534
- 348453866784
- 234066291263
- 054150576743

Recommendation:

It is recommended to enable AWS config.

When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (SNS), so that you are notified of all the configuration changes

Using AWS Config, you can quickly troubleshoot operational issues by identifying the recent configuration changes to your resources.

References:
Setting up AWS Config
AWS Config

Remediation Plan:

SOLVED: AWS CONFIG has been enabled.

3.7 (HAL-07) AUDIT AND LOGGING - LACK OF ELBV2 ACCESS LOGS - INFORMATIONAL

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.

Note that for Network Load Balancers, access logs are created only if the load balancer has a TLS listener.

Affected Resources:

- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-rpc/313f3547240b539e
- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-api-alb/db87f81801bc465a
- arn:aws:elasticloadbalancing:us-east-2:234066291263:loadbalancer/app/moonbase-api-alb/2cd9301f79798ba7
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-api-alb/6933a3686e70cd1c
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-rpc/c3d2cb59d7277688

Recommendation:

It is recommended enabling access logs to application load balancers where you want to parse and analyze logs for further security analysis.

1. Select the Load Balancer where you want to enable access logs.
2. Under the Description, select Edit Attributes.

3. Enable Access Logs.
4. Select S3 bucket to store the logs.
5. Make sure the S3 bucket permissions are set properly.

References:
Access logs for your Application Load Balancer
Access logs for your Network Load Balancer
Bucket permissions for access logs

Remediation Plan:

SOLVED: The Moonwell team has decommissioned all load balancers and no longer run any ELBv2 instances in any of their accounts. In the future, if they provision ELBs, they will enable access logging for them.

3.8 (HAL-08) DATA PROTECTION AND ENCRYPTION - LOAD BALANCER ALLOWING CLEAR TEXT (HTTP) COMMUNICATION - HIGH

Description:

HTTP by default provides no security and sends all the data in plain text over the wire, making your application vulnerable to HTTP sniffing.

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.

Affected Resources:

- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-rpc/313f3547240b539e
- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-api-alb/db87f81801bc465a
- arn:aws:elasticloadbalancing:us-east-2:234066291263:loadbalancer/app/moonbase-api-alb/2cd9301f79798ba7
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-api-alb/6933a3686e70cd1c
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-rpc/c3d2cb59d7277688

Recommendation:

It is recommended that your HTTP listener should redirect the traffic to your HTTPS listener instead.

References:
Redirect HTTP to HTTPS

Remediation Plan:

SOLVED: The Moonwell team has decommissioned all load balancers and no longer run any ELBv2 instances in any of their accounts. This cleartext communication was only enabled for a temporary purpose (so the CloudFlare CDN could access an origin and cache it without a self-signed certificate), and is no longer required.

3.9 (HAL-09) DATA PROTECTION AND ENCRYPTION - EBS VOLUMES NOT ENCRYPTED - MEDIUM

Description:

Unencrypted EBS volumes mean that data stored in your AWS EBS volumes might be at risk of potential security attack

Affected Resources:

- arn:aws:ec2:us-east-2:615885558947:volume/vol-080ba0870b5d1842c
- arn:aws:ec2:us-east-2:615885558947:volume/vol-08a9ac912dd360f45
- arn:aws:ec2:us-east-1:234066291263:volume/vol-0a2c7b0ffee475dc9
- arn:aws:ec2:us-east-2:234066291263:volume/vol-00b202de2bb852fdf
- arn:aws:ec2:us-east-2:054150576743:volume/vol-0486eea695cbd4fb7
- arn:aws:ec2:us-east-2:054150576743:volume/vol-090505593e39ae50c

Recommendation:

Enable encryption of your EBS volumes with a Customer Master Key (CMK).

References:
Best Practices for EBS Encryption
EBS Encryption

Remediation Plan:

SOLVED: These EC2 instances were only temporarily necessary and housed no proprietary data (they were Moonbeam blockchain nodes, so they only held publicly accessible blockchain data). There was no need to encrypt their EBS volumes since the data housed on them was publicly accessible. They have since been decommissioned and the unencrypted volumes have all been deleted.

It is a good practice to encrypt EBS volumes whenever proprietary/non-public data will be stored on them.

3.10 (HAL-10) DATA PROTECTION AND ENCRYPTION - EBS SNAPSHOT NOT ENCRYPTED - MEDIUM

Description:

Unencrypted EBS snapshots mean that data stored in your AWS EBS snapshots might be at risk of potential security attack

Affected Resources:

- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-005c8c3e20293f08c
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-006913eb51ac01687
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-01190a2c9c05bc136
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0152eed3d9c8e20c5
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0162c605bb78ac3a9
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0177ba5250a56ed5a
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-019413eddf183badb
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-01f26d0eb88bcf55b
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-022cef748f91e8ee5
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-023502fae481f8821
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-02c943250f279fbf6
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-02f31fdeb57864d11
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0367ba90682fb0dc5
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0370533763453c6e1
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-037145badf85f706f
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-03aeb423b2f6f071d
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-03cdd813116a6c516
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-03d930cc71125bb92
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-043b3280fe70b1f1c
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-047c5f9125a4018ab
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-04b522f7e0b499f32
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-053a61b82b107f771
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-053ff792e617c2951
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0570dd7889d184f1f

- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0587158cf6f965bec
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-05d119f2026e370f1
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-061d8cb5fbfbaeebc
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-06224b3dfb4d98f49
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-062b7d585c699c88f
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-06b7638553acd7ee1
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-07302bf2c8bdc77cb
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0798922403c35ffb4
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-07d1251f6411fddcf
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-07d81dd777c4e055f
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-092a4a13da5c9544b
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-09f9ccc24dce0912c
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0acbbbc20683af11e
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0afd12db04e072c64
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0b71005f9616746fc
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0bcd0e2fbb79c9d54
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0c816d1b16be608c8
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0c9e82e7d6e5280ea
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0cb4cbc7d161a49da
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0d8fcd6791d659c44
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0e860e51aa858df86
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0ec7265b1e29c4d80
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0ecf3a5f0b588222c
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0ed5d166c602e6451
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0ed968e4c18739669
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0f0f08eb75774d723
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0f3e0a1f51e855365
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0f4ac935bf50d63b4
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0fb9a65ddc3daeb7d
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0fdd9ba71d80363dc
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0fdf6af7a0877279f
- arn:aws:ec2:us-east-2:615885558947:snapshot/snap-0fdf98936b1d196c9

Recommendation:

Ensure that the AWS EBS volume snapshots that hold sensitive and critical data are encrypted to fulfill compliance requirements for data-at-rest

encryption using a Customer Master Key (CMK)

In order to encrypt and unencrypted snapshot, you must copy the unencrypted snapshot and enable encryption on the new copy.

References:
Copy EBS snapshot

Remediation Plan:

SOLVED: These snapshots were from EC2 instances that were only temporarily necessary and housed no proprietary data (they were Moonbeam blockchain nodes, so they only held publicly accessible blockchain data). There was no need to encrypt their EBS volumes since the data housed on them was publicly accessible. They have since been decommissioned and the unencrypted volumes and all snapshots generated from them have been deleted.

3.11 (HAL-11) DATA PROTECTION AND ENCRYPTION - LACK OF DELETION PROTECTION - MEDIUM

Description:

The following load balancers lack of deletion protection, which does not protect your lb from deletion mistakenly or intentionally.

Affected Resources:

- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-api-alb/6933a3686e70cd1c
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-rpc/c3d2cb59d7277688
- arn:aws:elasticloadbalancing:us-east-2:234066291263:loadbalancer/app/moonbase-api-alb/2cd9301f79798ba7
- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-rpc/313f3547240b539e
- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-api-alb/db87f81801bc465a

Recommendation:

It is recommended enabling deletion protection on the load balancers that have critical applications behind, enabling deletion protection on load balancers mitigates risks of accidental deletion.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. On the navigation pane, under LOAD BALANCING, choose Load Balancers.
3. Select the load balancer.
4. On the Description tab, choose Edit attributes.
5. On the Edit load balancer attributes page, select Enable for Delete Protection, and then choose Save.
6. Choose Save.

References:
Enable ALB Deletion Protection

Remediation Plan:

SOLVED: The Moonwell team has decommissioned all load balancers and no longer run any ELBv2 instances in any of their accounts. In the future, if they provision ELBs, they will enable deletion protection for them.

3.12 (HAL-12) DATA PROTECTION AND ENCRYPTION - EBS DEFAULT ENCRYPTION DISABLED - MEDIUM

Description:

If not enabled, sensitive information at rest is not protected.

Recommendation:

Enable EBS default encryption. Use a CMK where possible. It will provide additional management and privacy benefits, by enabling the default encryption you will make sure that any new EBS volume will be created with encryption by default.

References:
Turn on automatic encryption of new Amazon EBS

Remediation Plan:

RISK ACCEPTED: The Moonwell team does not currently have any EBS volumes, or intend to create any in the near future. We tend to avoid using EBS and EC2 wherever possible, and when we do use EBS and EC2, they are only for blockchain nodes that hold publicly accessible data that does not benefit from encryption at rest.

It is a good practice to encrypt EBS volumes whenever proprietary/non-public data will be stored on them.

3.13 (HAL-13) DATA PROTECTION AND ENCRYPTION - CONFIGURE AN AWS BACKUP PLAN - INFORMATIONAL

Description:

Use AWS Backup to centralize and automate data protection across AWS services and hybrid workloads.

AWS Backup could help you meet regulatory compliance for data protection by automating backups in a centralized place, these are the service that could be backed up with AWS Backup:

- Amazon Elastic Compute Cloud (Amazon EC2)instances
- Windows Volume Shadow Copy Service (VSS)supported applications (including Windows Server, Microsoft SQL Server, and Microsoft Exchange Server)on Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)volumes
- Amazon Simple Storage Service (Amazon S3)buckets
- Amazon Relational Database Service (Amazon RDS)databases (including Amazon Aurora clusters)
- Amazon DynamoDB tables
- Amazon Neptune databases
- Amazon DocumentDB (with MongoDB compatibility)databases
- Amazon Elastic File System (Amazon EFS)file systems
- Amazon FSx for NetApp ONTAP file systems
- Amazon FSx for Lustre file systems
- Amazon FSx for Windows File Server file systems
- Amazon FSx for OpenZFS file systems
- AWS Storage Gateway volumes
- VMware workloads on premises, on Amazon Outposts, and in VMware CloudTM on AWS

Recommendation:

It is recommended configuring an AWS backup plan to improve your backup compliance by automating the backup process of several services within a centralized place.

References:
AWS Backup
AWS Backup features

Remediation Plan:

RISK ACCEPTED: The Moonwell team are not currently using any of the services that are supported by AWS Backup. In the future, if they use a service, such as S3, EBS, RDS, or DynamoDB, that is supported by AWS Backup, Halborn will configure a plan.

3.14 (HAL-14) DETECTION AND MONITORING - SCAN ON PUSH DISABLED ON ECR - MEDIUM

Description:

Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project and provides a list of scan findings.

Affected Resources:

- 054150576743.dkr.ecr.us-east-2.amazonaws.com/moonbeam-api-repository-ryhqkqa0jtcx
- 054150576743.dkr.ecr.us-east-2.amazonaws.com/moonbeam-statistics-collector-repository-tijjlyhulgrj
- 234066291263.dkr.ecr.us-east-2.amazonaws.com/moonbase-api-repository-4gprfmmgmrol
- 234066291263.dkr.ecr.us-east-2.amazonaws.com/moonbase-collector-repository-hdtklqsyxtpf
- 615885558947.dkr.ecr.us-east-2.amazonaws.com/moonriver-api-repository-qfokt6o1m9z3
- 615885558947.dkr.ecr.us-east-2.amazonaws.com/moonriver-statistics-collector-repository-ykr95pe5q4bc

Recommendation:

Enable ECR image scanning and review the scan findings for information about the security of the container images that are being deployed.

References:
Image scanning

Remediation Plan:

SOLVED: Remediated on Cloudformation template that using as a starting point for most containerized services.

3.15 (HAL-15) IAM - WEAK PASSWORD POLICY - HIGH

Description:

The password policy did not enforce strong password policy. As a result, password complexity requirements were not in line with security best practice. Your passwords could be rapidly guessed by executing a brute force attack using a subset of all possible passwords. Since password expiration is disabled, compromised credentials could be used by potential attackers for an indefinite amount of time.

Affected Resources:

- Account id: 054150576743
- Account id: 234066291263
- Account id: 348453866784

- Account id: 409295697534
- Account id: 615885558947

Listing 3: Password policy

```
1 Minimum password length: 1 It should be noted that 1 character
↳ passwords are authorized when no password policy exists, even
↳ though the web console displays "6".
2 Require at least one uppercase letter: false
3 Require at least one lowercase letter: false
4 Require at least one number: false
5 Require at least one non-alphanumeric character: false
6 Enable password expiration: false
7 Prevent password reuse: false
```

Risk Level:

Likelihood - 4

Impact - 4

Recommendation:

Ensure the password policy is configured to:
Enforce password complexity as per recommendation
Enable password expiration
Prevent password reuse

References:
- Setting an account password policy for IAM users

Remediation Plan:

PARTIALLY SOLVED: There is only a single account that holds user accounts in our organization: the IAM account. All other accounts only hold roles that must be assumed by a user in the IAM account.

3.16 (HAL-16) IAM - ROOT ACCOUNT USED RECENTLY - HIGH

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.

Affected Accounts:

- 348453866784

Recommendation:

Minimizing the use of this account and adopting the principle of least privilege for access management reduces the risk of accidental changes and unintended disclosure of highly privileged credentials.

References:
Avoid the use of the “root” account

Remediation Plan:

SOLVED: The root account was only used during the initial setup of the AWS Organization master account and creation of all subaccounts, users in the IAM account, and roles in the subaccounts. Once the setup is done, the root password and MFA seed have been vaulted and should only be used in the event of loss of access to all user accounts.

3.17 (HAL-17) NETWORK SECURITY - DEFAULT VPC BEING USED - CRITICAL

Description:

The default VPC lacks the proper security and auditing controls, using default vpc means that all of your resources are being deployed into public subnets since default vpc does not have private subnets or nat gateways.

Affected Resources:

Resources on the following accounts:

- 054150576743
- 234066291263
- 615885558947

Recommendation:

Create a new VPC with three layers of subnets; public, private and data subnets, only services that should be accessible from the internet should be hosted on public subnets such as load balancers, this will mitigate the risk of Denial-of-Service (DOS) Attack, Password Attack, Brute force attack, port scanning and others.

References:
Security in Amazon Virtual Private Cloud

Remediation Plan:

RISK ACCEPTED: There is nothing inherently wrong with using the default VPC. It is simply a VPC with 3 public subnets in it. Of course, we follow best practices including least privilege, and do not open security groups unnecessarily, which prevents non-public access. For secure workloads

that might require private subnets, we provision dedicated VPCs with both public and private subnets, and use managed NAT gateways to enable outbound access (where appropriate).

3.18 (HAL-18) NETWORK SECURITY - SECURITY GROUP OPENS SSH PORT TO ALL - CRITICAL

Description:

The security group was found to be exposing a well-known 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 the Internet. If such services need to be exposed, a restriction on the source address could help to reduce the attack surface of the infrastructure.

Affected Resources:

- arn:aws:ec2:us-east-2:054150576743:security-group/sg-06e400e8d619733c1
- arn:aws:ec2:us-east-1:234066291263:security-group/sg-0d2258bda0169d75c
- arn:aws:ec2:us-east-2:234066291263:security-group/sg-0ccf4490a4e0a9c31
- arn:aws:ec2:us-east-2:615885558947:security-group/sg-04e55ef34a4297443
- arn:aws:ec2:us-east-2:615885558947:security-group/sg-05f127b527658da5b

Recommendation:

Set a more restrictive CIDR range.

Remediation Plan:

SOLVED: The systems that required SSH access have all been decommissioned and we no longer have any EC2 instances running in any of our accounts.

These systems were only temporary, and housed no non-public data, so security was not as much of a concern, however, it is our general practice to never open SSH to 0.0.0.0/0 or any wide CIDR blocks.

3.19 (HAL-19) NETWORK SECURITY - RDS PUBLICLY ACCESSIBLE ENABLED - CRITICAL

Description:

RDS publicly accessible means that the RDS is reachable through the internet and a public IP will be assigned, even though you might be restricting access with security groups, this option should not be enabled, since a security group port could be opened mistakenly and will expose the RDS public IP.

Affected Resources:

- arn:aws:rds:us-east-2:054150576743:db:moonbeam-collector-db
- arn:aws:rds:us-east-2:234066291263:db:moonbase-collector-db
- arn:aws:rds:us-east-2:615885558947:db:moonriver-collector-db

Recommendation:

Only your internal services should be able to access your RDS instance. Make sure that no public IPS are being assigned to your RDS instance by disabling the Publicly Accessible setting.

If the database is on a public subnet, move your resources to a private subnet instead.

References:
- Move an Amazon RDS DB instance from a public subnet to private subnet

Remediation Plan:

SOLVED: These RDS database instances have all been decommissioned, and only housed publicly accessible data. The Moonwell team enabled public accessibility so that we could run SQL queries remotely, and restricted

the access to specific /32 CIDR blocks of our source IPs.

3.20 (HAL-20) NETWORK SECURITY - DROP INVALID HEADER FIELDS DISABLED - MEDIUM

Description:

The following load balancers does not have drop invalid header fields enabled; therefore invalid headers could be sent to your application.

Affected Resources:

- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-rpc/313f3547240b539e
- arn:aws:elasticloadbalancing:us-east-2:054150576743:loadbalancer/app/moonbeam-api-alb/db87f81801bc465a
- arn:aws:elasticloadbalancing:us-east-2:234066291263:loadbalancer/app/moonbase-api-alb/2cd9301f79798ba7
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-api-alb/6933a3686e70cd1c
- arn:aws:elasticloadbalancing:us-east-2:615885558947:loadbalancer/app/moonriver-rpc/c3d2cb59d7277688

Recommendation:

Dropping invalid header fields should be enabled to mitigate the risk of request smuggling attacks.

Please enable drop invalid header fields attribute to your load balancers:

- Identify the load balancer you want to modify on the AWS Console
- Select the Description tab and click on the Edit attributes button available in the Attributes section.
- Select the Drop Invalid Header Fields configuration checkbox to enable the Drop Invalid Header Fields security feature for the selected Application Load Balancer.

References:

HTTP Desync Attacks with Python and AWS

Request smuggling between Amazon ALBs and Go net/http

HTTP request smuggling

Remediation Plan:

SOLVED: We have decommissioned all of these load balancers, and no longer run any ELB instances in our AWS accounts. In the future, if we provision load balancer resources, we will enable dropping invalid header fields.

3.21 (HAL-21) NETWORK SECURITY - UNUSED SECURITY GROUPS - LOW

Description:

It is important to ensure that any unused security groups, i.e., the ones not attached to any instance, are deleted immediately. Deleting unused security groups not only keeps your AWS environment clean, but it also ensures that unused security groups are not accidentally attached to any instance, inadvertently opening up your environment to attacks

Affected Resources:

- arn:aws:ec2:us-east-2:615885558947:security-group/sg-04e55ef34a4297443
- arn:aws:ec2:us-east-2:054150576743:security-group/sg-03bc96a33e8f58f10

Recommendation:

Delete any unused security groups

Remediation Plan:

SOLVED: All unused security groups have been removed.

THANK YOU FOR CHOOSING

// HALBORN