

VM VULNERABILITY ASSESSMENT REPORT

-Group 26

EXECUTIVE SUMMARY

The study on Amazon Web Services (AWS) VM Vulnerability Assessment offers a thorough brief of the security stance in the company's VM environment. The assessment aimed to identify any gaps, misconfigurations, and vulnerabilities that would jeopardize the integrity of the cloud infrastructure. Overall, the evaluation showed that strong network restrictions and properly configured security groups were in place, demonstrating a praiseworthy adherence to AWS security best practices. Despite the largely strong security foundation, a few potential trouble spots were found. These include infrequent occurrences of unpatched systems and out-of-date software versions, which could provide possible entry points for bad actors. Furthermore, even with strong authentication procedures, sporadic instances of incorrectly configured access policies and permissions were found, highlighting the necessity of constant watchfulness. By adopting these preventative measures, the company may strengthen the AWS environment's defenses against possible cyberattacks and protect the integrity, confidentiality, and availability of vital cloud-hosted assets and services.

SUMMARY OF FINDINGS

Severity	Security Misconfiguration/Vulnerabilities
High	<ul style="list-style-type: none">- Database Username minimum length is set to '1.'- Volume is not Encrypted.- Kernel Vulnerabilities- Usage of port 80 and 22
Medium	<ul style="list-style-type: none">- ACL all Ports access- VPC Group does not restrict all traffic.- Disabled IMDSv2

Database Username minimum length is set to '1.' 

Description: Database Username minimum length is set to '1'


Severity: High

```
DBUsername:
  NoEcho: 'true'
  Description: Username for MySQL database access
  Type: String
  MinLength: '1'
  MaxLength: '16'
  AllowedPattern: '[a-zA-Z][a-zA-Z0-9]*'
  ConstraintDescription: must begin with a letter and contain only alphanumeric characters.
  Default: doctorenmp665
```

Potential Impact:

Allowing a username with a minimum length of '1' means that users can set very short and simple usernames. This makes it easier for attackers to guess or brute force usernames, increasing the risk of unauthorized access.

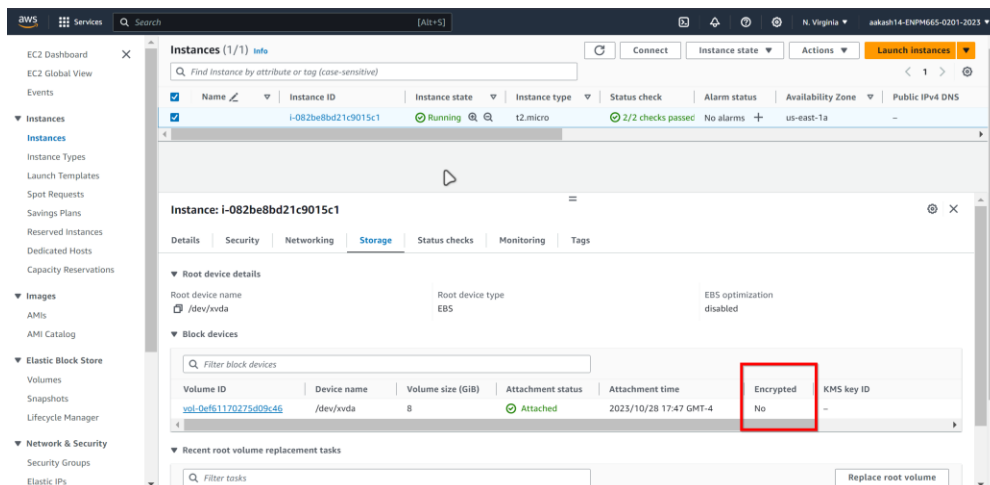
Remediation:

Increase username minimum length from 1 to 6 or more. 

Volume is not Encrypted.

Description: EC2 volume is not encrypted

Severity: High



The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area displays the details for an EC2 instance named 'i-082be8bd21c9015c1'. The 'Storage' tab is selected, showing the root device details. The root device is an EBS volume named '/dev/xvda' with a size of 8 GiB. The 'Encrypted' checkbox is unchecked, indicating the volume is not encrypted. A red box highlights the 'Encrypted' field.

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-0ef61170275d09c46	/dev/xvda	8	Attached	2023/10/28 17:47 GMT-4	No	-

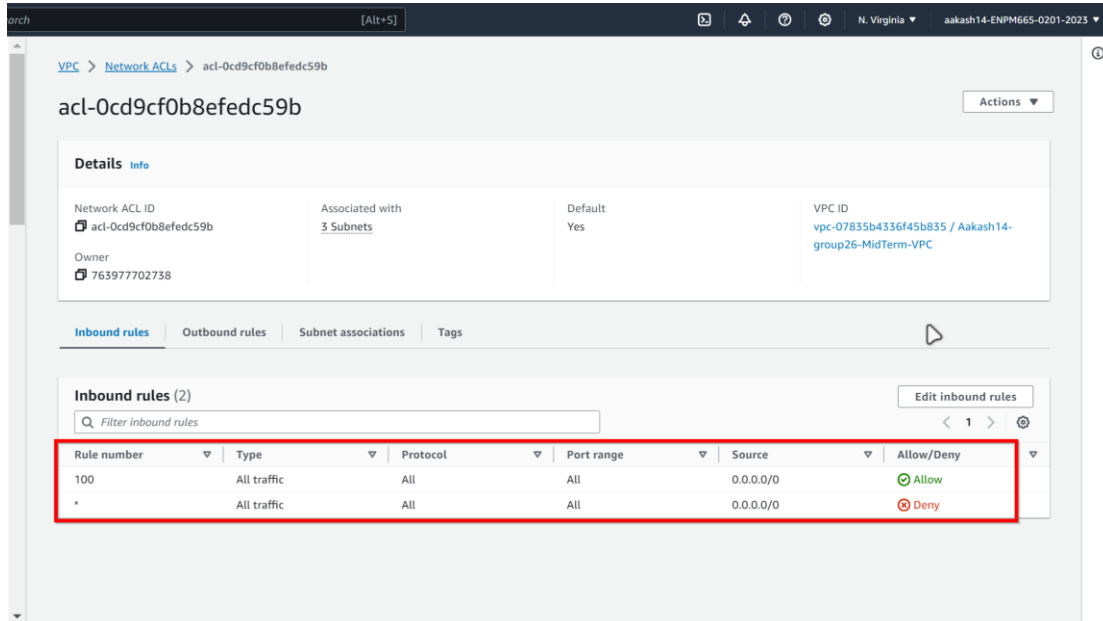
Potential Impact:

Since we are dealing with the Health Records of the patients, we need to make sure that we are encrypting the volumes, since this data is highly confidential. If attackers get to this volume, they will be able to access all the PII (Personally Identifiable Information) of the patients.

ACL all Ports access

Description: ACL has allowed all ports in Inbound rules

Severity: Medium



Potential Impact:

ACL allows all ports to be accessed from all traffic. This is not a good sign, as we can access all ports from the internet, as this increases the attack surface.

Remediation:

Block access to the ports and only give access to some important ports from some important addresses.

Kernel Vulnerabilities and other similar vulnerabilities

Description: Different kernel vulnerabilities found via Amazon Inspector

Severity: High

Potential Impact:

There are a lot of high severity vulnerabilities with a lot of serious CVEs. If we were to access them from the internal side, do a privilege escalation, then it can cause major trouble.

Amazon - Inspector Findings:

Dashboard

Findings

By vulnerability

By instance

By container image

By container repository

By Lambda function

All findings

Export SBOMs

Suppression rules

Vulnerability database search

Account management

General settings

EC2 scanning settings

ECR scanning settings

Usage

Video tutorials

What's New 14

Switch to Inspector Classic

Findings: All findings info

All findings ranked by severity.

Findings (298)

Choose a row to see the finding details.

Findings status

Active

Filter criteria

Add filter

Export findings

Create suppression rule

Severity	Title	Impacted resource	Type	Age	Status
High	CVE-2021-42574 - libstdc++ - libgcc and 1	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-28466 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-29581 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2019-19816 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-45934 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-32399 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-1966 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2019-19060 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-3653 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-33200 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active

CloudShell

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Dashboard

Findings

By vulnerability

By instance

By container image

By container repository

By Lambda function

All findings

Export SBOMs

Suppression rules

Vulnerability database search

Account management

General settings

EC2 scanning settings

ECR scanning settings

Usage

Video tutorials

What's New 14

Switch to Inspector Classic

High	CVE-2023-3776 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-1838 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-3090 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-30594 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-22555 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-3609 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-2978 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-1679 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-3621 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-3518 - libxml2-python - libxml2	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-3524 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-44733 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2021-27365 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-4622 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-0435 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-4208 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-3390 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2023-1281 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active

CloudShell

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

High	CVE-2023-1281 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-40303 - libxml2-python - libxml2	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
High	CVE-2022-26365 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active

○	■ High	CVE-2023-1829 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-1586 - pcre2	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-26930 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2020-25670 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-28772 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-1206 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-27666 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-1011 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2020-27815 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-33034 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-27405 - freetype	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-4206 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2020-29361 - p11-kit-trust, p11-kit	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-3347 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-38185 - cpio	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-20141 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-2588 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-4207 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2020-16119 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2020-25671 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-27406 - freetype	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2018-25020 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-27384 - mariadb-libs	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-3565 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-28390 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-0045 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2023-3611 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-3517 - libxml2-python, libxml2	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2021-3348 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active
○	■ High	CVE-2022-36123 - kernel	i-082be8bd21c9015c1	Package Vulnerability	an hour	Active

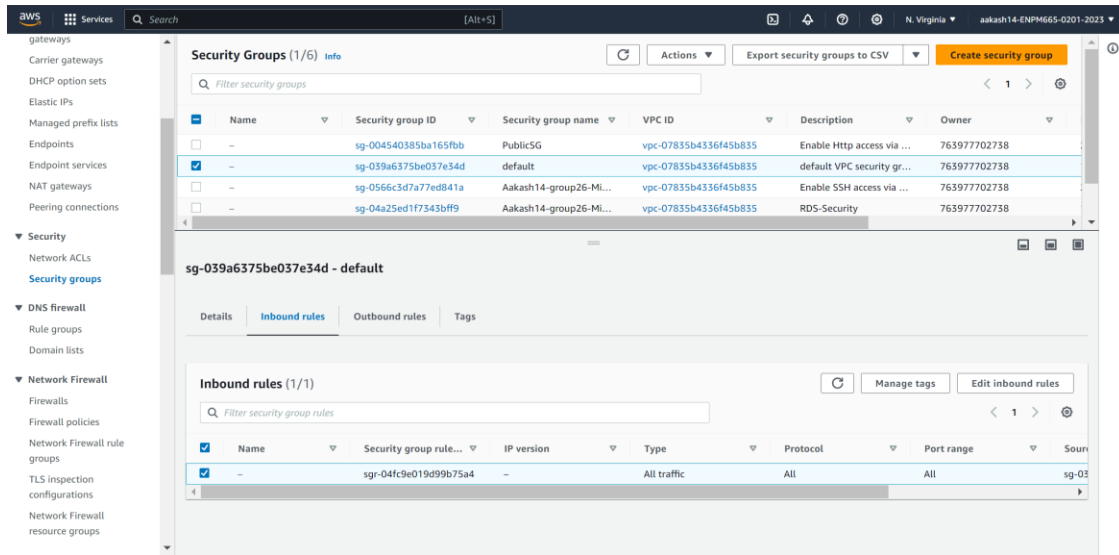
Remediation:

Update the generic software, and the python modules.

VPC Group not restricting all traffic:

Description: Default VPC group not restricting traffic and giving access to all ports.

Severity: Medium



Potential Impact:

This increases the chance of attacks on EC2 instance and unnecessary risk too. This also increases the chance of data exposure.

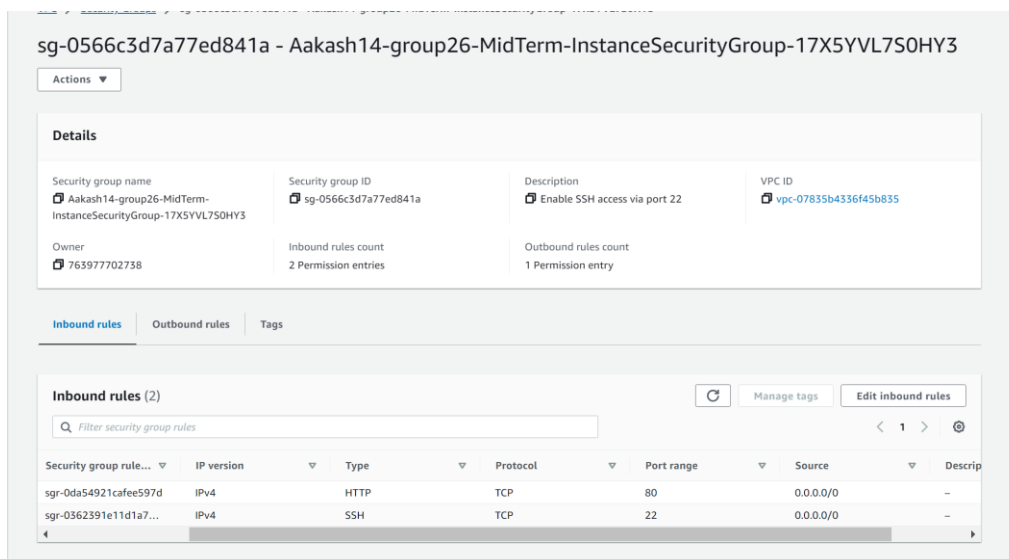
Remediation:

We can create custom security groups and restrict inbound and outbound traffic. Additionally, we can also update the security rules.

Usage of port 80 and 22:

Description: We are allowing port access to SSH port – 22 and using HTTP port – 80

Severity: High



Potential Impact:

Allowing all traffic to connect to the SSH port is a very bad idea. Using port 80 for HTTP is not a good practice as all the data is unencrypted and can be seen in clear text if intercepted.

Remediation:

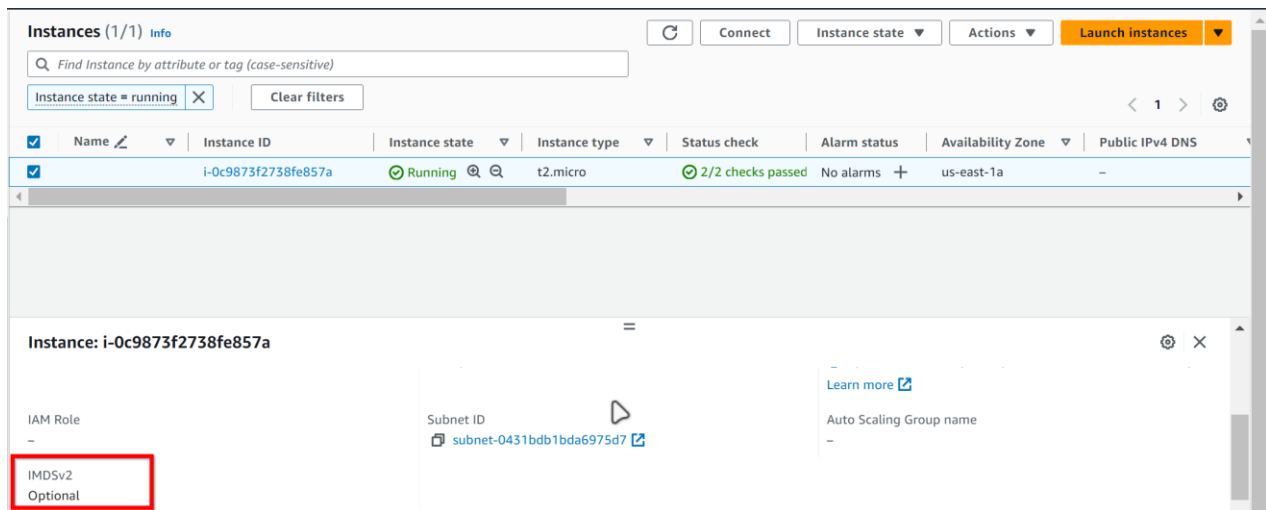
We need to allow access to the SSH port only from trusted IP address and keep it as many minimal addresses as possible.

We need to use port 443 for website traffic to start using HTTPS instead of HTTP.

IMDSv2 is disabled.

Description: IMDSv2 is disabled on the EC2 instance

Severity: Medium

**Potential Impact:**

Disabling IMDSv2 in EC2 instance can lead to security attacks such as token theft or data manipulation. It could further lead to unauthorized access or data exposure.

Remediation:

Enable IMDSv2 on the EC2 instance using AWS console/CLI from your PC.

