



Amazon Inspector - Assessment Report

Findings Report

Report generated on 2021-12-12 at 01:07:53 UTC

Assessment Template: Assessment-Template-Default-All-Rules

Assessment Run start: 2021-12-11 at 14:04:33 UTC

Assessment Run end: 2021-12-11 at 14:05:20 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2021-12-11 14:04:33 UTC for assessment template 'Assessment-Template-Default-All-Rules'. The assessment target included 2 instances, and was tested against 1 Rules Packages.

The assessment target is defined using the following EC2 tags

| Key | Value |
|-----|-------|
|-----|-------|

The following Rules Packages were assessed. A total of 1 findings were created, with the following distribution by severity:

| Rules Package | High | Medium | Low | Informational |
|--------------------------|------|--------|-----|---------------|
| Network Reachability-1.1 | 0 | 0 | 0 | 1 |

Section 2: What is Tested

This section details the Rules Packages included in this assessment run, and the EC2 instances included in the assessment target.

2.1: Rules Packages - Count: 1

2.1.1: Network Reachability-1.1

Description: These rules analyze the reachability of your instances over the network. Attacks can exploit your instances over the network by accessing services that are listening on open ports. These rules evaluate the security your host configuration in AWS to determine if it allows access to ports and services over the network. For reachable ports and services, the Amazon Inspector findings identify where they can be reached from, and provide guidance on how to restrict access to these ports.

Provider: Amazon Web Services, Inc.

Version: 1.1

2.2: Assessment Target - Assessment-Template-Default-All-Rules

2.2.1: EC2 Tags:

The following EC2 tags (Key/Value pairs) were used to define this assessment target.

| Key | Value |
|-----|-------|
|-----|-------|

2.2.2: Instances - Count 2

| Instance ID |
|---------------------|
| i-06c4eea6eadb11e51 |
| i-090ecb336e8e80ce2 |

Section 3: Findings Summary

This section lists the rules that generated findings, the severity of the finding, and the number of instances affected. More details about the findings can be found in the "Findings Details" section. Rules that passed on all target instances available during the assessment run are listed in the "Passed Rules" section.

3.1: Findings table - Network Reachability-1.1

| Rule | Severity | Failed |
|--------------------------------------------------|---------------|--------|
| TCP port 22 (SSH) is reachable from the internet | Informational | 1 |

Section 4: Findings Details

This section details the findings generated in this assessment run, and the instances that generated the finding. If an instance is not listed here, that means it was checked and passed.

4.1: Findings details - Network Reachability-1.1

TCP port 22 (SSH) is reachable from the internet

Severity

Informational

Description

On this instance, recognized port(s) are reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port.

Recommendation

You can edit the Security Group sg-0f3897fb33253127b to remove access from the internet on port 22

Failed Instances

i-06c4eea6eadb11e51