Amazon Inspector - Assessment Report

Findings Report

Report generated on 2024-08-14 at 09:12:19 UTC

Assessment Template: PH-LTI-SVR

Assessment Run start: 2024-08-14 at 07:09:31 UTC
Assessment Run end: 2024-08-14 at 08:12:32 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2024-08-14 07:09:31 UTC for assessment template 'PH-LTI-SVR'. The assessment target included 1 instances, and was tested against 3 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Name	PH-LTI-SVR06

The following Rules Packages were assessed. A total of 3 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
Common Vulnerabilities and Exposures-1.1	0	0	0	0
Network Reachability-1.1	0	0	0	0
Security Best Practices-1.0	0	3	0	0

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: 3

2.1.1: Common Vulnerabilities and Exposures-1.1

Description: The rules in this package help verify whether the EC2 instances in your application are exposed to Common Vulnerabilities and Exposures (CVEs). Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference for publicly known information security vulnerabilities and exposures. For more information, see https://cve.mitre.org/. If a particular CVE appears in one of the produced Findings at the end of a completed Inspector assessment, you can search https://cve.mitre.org/ using the CVE's ID (for example, "CVE-2009-0021") to find detailed information about this CVE, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.2: 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

2.1.3: Security Best Practices-1.0

Description: The rules in this package help determine whether your systems are configured securely.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.2: Assessment Target - PH-LTI-SVR

2.2.1: EC2 Tags:

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

Key	Value
Name	PH-LTI-SVR06

2.2.2: Instances - Count 1

Instance ID
i-059655ae04e7f94da

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 - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

3.2: Findings table - Network Reachability-1.1

No findings were generated for this rules package.

3.3: Findings table - Security Best Practices-1.0

Rule	Severity	Failed
Configure Password Complexity	Medium	1
Disable Password Authentication Over SSH	Medium	1
Disable root login over SSH	Medium	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 - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

4.2: Findings details - Network Reachability-1.1

No findings were generated for this rules package.

4.3: Findings details - Security Best Practices-1.0

Configure Password Complexity

Severity
Medium

Description
This rule helps determine whether a password complexity mechanism is configured on your EC2 instances.

Recommendation
If you are using passwords, it is recommended that you configure all EC2 instances in your assessment target to require a level of password complexity. You can do this by using pam_cracklib.so "lcredit", "ucredit", "dcredit", and "ocredit" settings. See man pam_cracklib for more information.

Failed Instances
i-059655ae04e7f94da

Disable Password Authentication Over SSH

Severity
Medium

Description
This rule helps determine whether your EC2 instances are configured to support password authentication over the SSH protocol.

Recommendation
It is recommended that you disable password authentication over SSH on your EC2 instances and enable support for key-based authentication instead. This significantly reduces the likelihood of a successful brute-force attack. For more information see https://aws.amazon.com/articles/1233/. If password authentication is supported, it is important to restrict access to the SSH server to trusted IP addresses.

Failed Instances
i-059655ae04e7f94da

Disable root login over SSH

Severity
Medium

Description
This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation
To reduce the likelihood of a successful brute-force attack, we recommend that you configure your EC2 instance to prevent root account logins over SSH. To disable SSH root account logins, set PermitRootLogin to 'no' in /etc/ssh/sshd_config and restart sshd. When logged in as a non-root user, you can use sudo to escalate privileges when necessary. If you want to allow public key authentication with a command associated with the key, you can set PermitRootLogin to 'forced-commands-only'.

Failed Instances
i-059655ae04e7f94da