Amazon Inspector - Assessment Report

Findings Report

Report generated on 2018-07-28 at 10:12:44 UTC

Assessment Template: Full-Scan

Assessment Run start: 2018-07-27 at 11:17:32 UTC
Assessment Run end: 2018-07-27 at 12:19:21 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2018-07-27 11:17:32 UTC for assessment template 'Full-Scan'. 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

The following Rules Packages were assessed. A total of 4 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
Common Vulnerabilities and Exposures-1.1	0	2	0	0
Runtime Behavior Analysis-1.0	0	0	0	1
Security Best Practices-1.0	0	1	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: Runtime Behavior Analysis-1.0

Description: These rules analyze the behavior of your instances during an assessment run, and provide guidance on how to make your instances more secure.
Provider: Amazon Web Services, Inc.
Version: 1.0

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 - Full-Scan

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 1

Instance ID
i-0c04c2696a3923a5c

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

Rule	Severity	Failed
CVE-2018-11412	Medium	1
CVE-2018-12232	Medium	1

3.2: Findings table - Runtime Behavior Analysis-1.0

Rule	Severity	Failed
Unused listening TCP ports	Informational	1

3.3: Findings table - Security Best Practices-1.0

Rule	Severity	Failed
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

CVE-2018-11412

Severity
Medium

Description
In the Linux kernel 4.13 through 4.16.11, ext4_read_inline_data() in fs/ext4/inline.c performs a memcpy with an untrusted length value in certain circumstances involving a crafted filesystem that stores the system.data extended attribute value in a dedicated inode.

Recommendation
Use your Operating System's update feature to update package kernel-0:4.14.47-56.37.amzn1, kernel-tools-0:4.14.47-56.37.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11412

Failed Instances
i-0c04c2696a3923a5c

CVE-2018-12232

Severity
Medium

Description
In net/socket.c in the Linux kernel through 4.17.1, there is a race condition between fchownat and close in cases where they target the same socket file descriptor, related

to the sock_close and sockfs_setattr functions. fchownat does not increment the file descriptor reference count, which allows close to set the socket to NULL during fchownat's execution, leading to a NULL pointer dereference and system crash.

Recommendation
Use your Operating System's update feature to update package kernel-0:4.14.47-56.37.amzn1, kernel-tools-0:4.14.47-56.37.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12232

Failed Instances
i-0c04c2696a3923a5c

4.2: Findings details - Runtime Behavior Analysis-1.0

Unused listening TCP ports

Severity
Informational

Description
This rule detects listening TCP ports that may not be required by the assessment target.

Recommendation
To reduce the attack surface area of your deployments, we recommend that you disable network services that you do not use. Where network services are required, we recommend that you employ network control mechanisms such as VPC ACLs, EC2 security groups, and firewalls to limit exposure of that service.

Failed Instances
i-0c04c2696a3923a5c

4.3: Findings details - Security Best Practices-1.0

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

It is recommended that you configure your EC2 instance to prevent root logins over SSH. Instead, log in as a non-root user and use sudo to escalate privileges when necessary. To disable SSH root logins, set PermitRootLogin to "no" in /etc/ssh/sshd_config and restart sshd.

Failed Instances

i-0c04c2696a3923a5c