Amazon Inspector - Assessment Report

Findings Report

Report generated on 2018-01-20 at 16:45:49 UTC

Assessment Template: PublicNetworkTemplate

Assessment Run start: 2018-01-20 at 15:22:24 UTC
Assessment Run end: 2018-01-20 at 16:24:07 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2018-01-20 15:22:24 UTC for assessment template 'PublicNetworkTemplate'. 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
Network	Public

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	1	0	0
Runtime Behavior Analysis-1.0	0	0	1	1
Security Best Practices-1.0	0	0	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 - PublicNetworkTemplate

2.2.1: EC2 Tags:

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

Key	Value
Network	Public

2.2.2: Instances - Count 1

Instance ID
i-0f07b189e6691ceae

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-2017-5754	Medium	1

3.2: Findings table - Runtime Behavior Analysis-1.0

Rule	Severity	Failed
Insecure client protocols (general)	Low	1
Unused listening TCP ports	Informational	1

3.3: Findings table - Security Best Practices-1.0

No findings were generated for this rules package.

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-2017-5754

Severity
Medium

Description
Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:2.6.32-431.11.2.el6, kernel-0:2.6.32-431.el6, kernel-0:3.10.0-327.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.4.35-33.55.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.51-10.52.amzn1, kernel-0:4.9.58-18.51.amzn1, kernel-devel-0:2.6.32-431.11.2.el6, kernel-firmware-0:2.6.32-431.11.2.el6, kernel-headers-0:2.6.32-431.11.2.el6, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:4.9.43-17.38.amzn1, kernel-tools-0:4.9.58-18.51.amzn1, kernel-tools-libs-0:3.10.0-327.el7, linux-image-4.4.0-1044-aws, linux-image-4.4.0-1044-aws-0:4.4.0-1044.53, linux-image-aws, linux-image-aws-0:4.4.0.1044.46-0, python-perf, python-perf-0:3.10.0-327.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754

Failed Instances
i-0f07b189e6691ceae

4.2: Findings details - Runtime Behavior Analysis-1.0

Insecure client protocols (general)

Severity
Low

Description
This rule detects client use of insecure protocols.

Recommendation
It is recommended that you replace these insecure protocols with encrypted versions.

Failed Instances
i-0f07b189e6691ceae

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-0f07b189e6691ceae

4.3: Findings details - Security Best Practices-1.0

No findings were generated for this rules package.