Amazon Inspector

Automating the *Sec* in *DevSecOps*

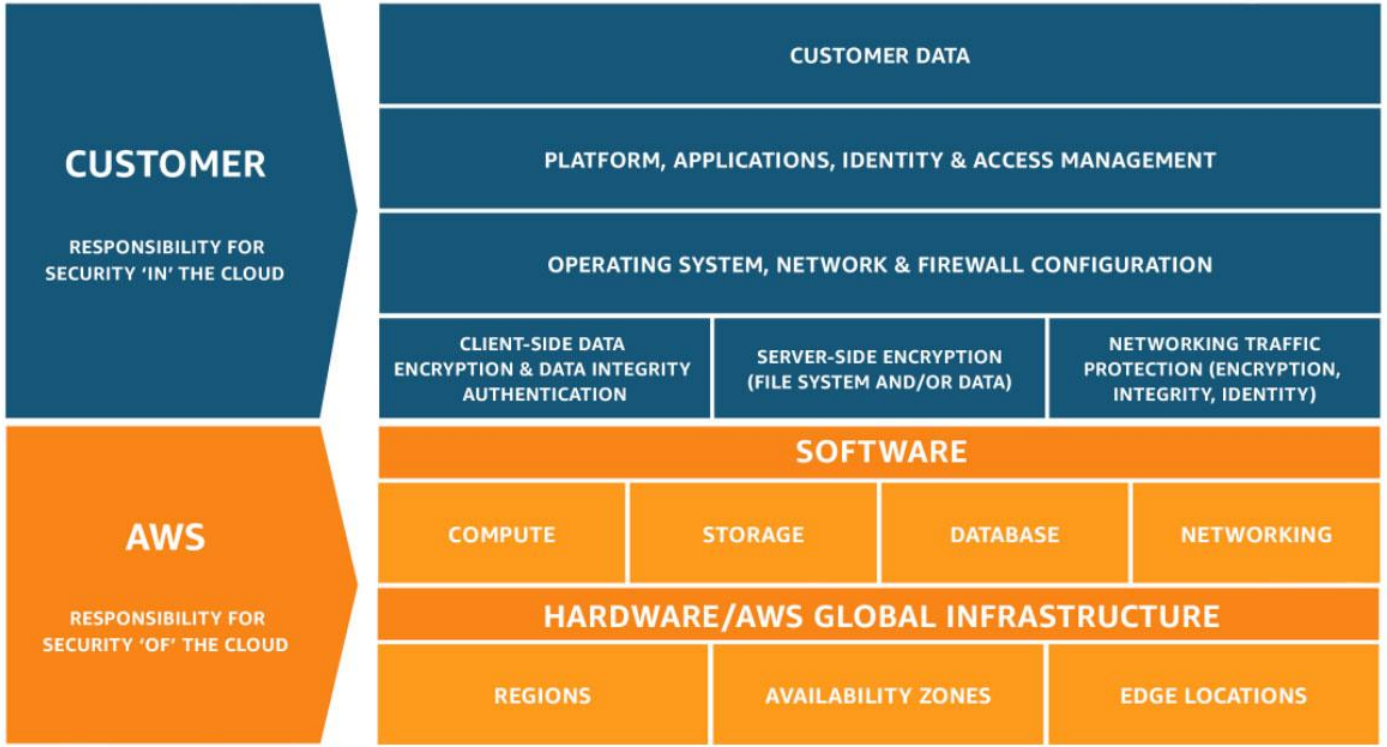
Catherine Dodge – Technical Program Manager

What are we going to do?

- Overview of Amazon Inspector
- Demo: How to assess your whole fleet quickly
- Demo: Tailoring your workflow
- Demo: Scaling vulnerability assessments in the cloud
- Wrap up

aws

Shared Security Model

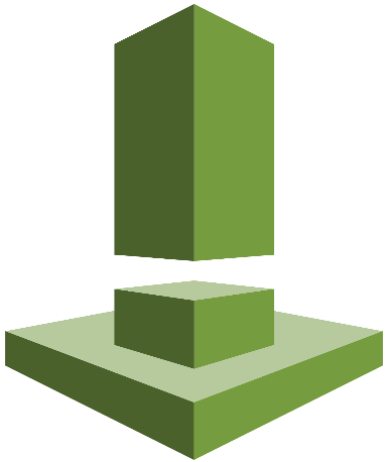


aws

Why launch Amazon Inspector?

Our customers asked us to:

- Complement Shared Security Model
- Automatable for DevSecOps
- Provide Recommendations

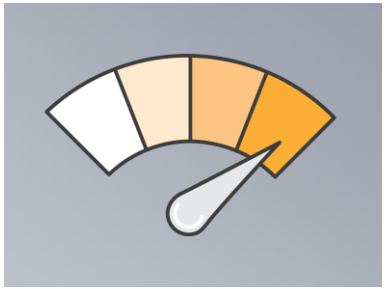


Am I Secure?

- Are my instances exposed to the latest vulnerabilities?
- Are my instances hardened for security?
- Are my instances password policies in line with best practices?
- Does my application use insecure protocols?

What is Amazon Inspector?

Simple
Vulnerability Assessment
for your Compute



Pay as you Go

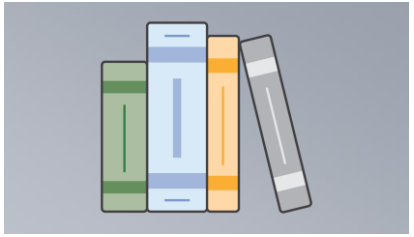
Integrate Security
into DevOps +
Production

aws

Key Concepts for Inspector

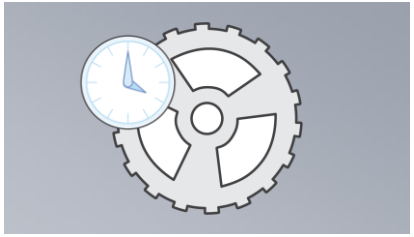
Assessment Template

Assessment Targets



Rules Packages

Inspector Agent

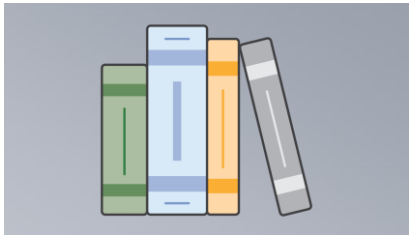


Triggers & Runs

Findings & Reports

aws

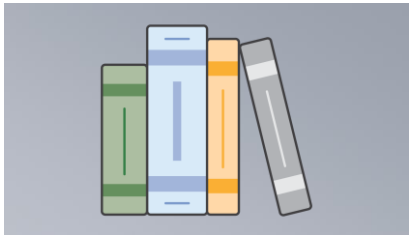
Amazon Inspector Rules Packages



- Common Vulnerabilities and Exposures (CVE)
- Center for Internet Security (CIS) benchmarks
- Security Best Practices
- Runtime Behavior Analysis

aws

Am I Secure?



- Are my instances exposed to the latest vulnerabilities?
- Are my instances hardened for security?
- Are my password policies in line with best practices?
- Does my application use insecure protocols?

Common Vulnerabilities and Exposures (CVE)

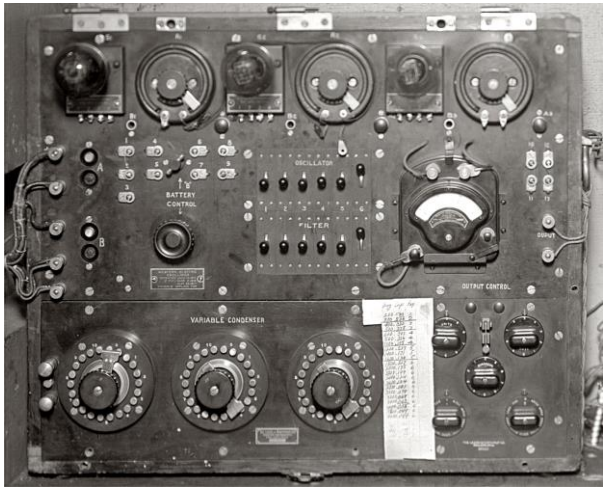
Center for Internet Security (CIS) benchmarks

Security Best Practices

Runtime Behavior Analysis

aws

Simple AND Customizable



aws

Demo 1: How to assess your whole fleet quickly

- Run against all instances with zero configuration
- Simple scheduling
- Agent installation via Systems Manager

Demo 2: Tailoring your workflow

- Tune the set of instances and rules
- Configuring a complex schedule
- Configuring notifications to apps
    - Send any **high** severity findings to Chime

Blog post: https://aws.amazon.com/blogs/aws/scale-your-security-vulnerability-testing-with-amazon-inspector/

Inspector -> SNS -> Chime

Inspector Test Alerts (Webhook) 10:50 PM

Title:
Instance i-0ad1bfa53f79e6936 is vulnerable to CVE-2017-17448

Description:
net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list data structure is shared across all net namespaces.

Recommendation:
Use your Operating System's update feature to update package linux-image-4.4.0-1052-aws-0:4.4.0-1052.61.
For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17448

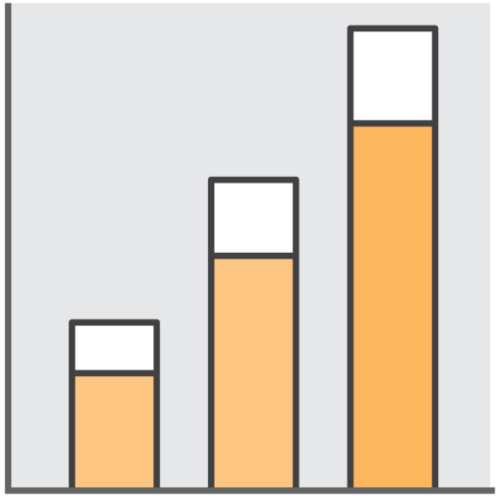
Demo 3: Scaling vulnerability assessments

- Use CloudFormation templates
- Auto-populate the Systems Manager Inventory
- Fleet Management Solution available at:

https://docs.aws.amazon.com/solutions/latest/server-fleet-management-at-scale/overview.html

Inspector Scales as you Grow

- Get started doing weekly assessments in minutes
- Tailor the workflow to your use cases
- Build into infrastructure as you grow



Supported Regions

Asia Pacific (Mumbai)
Asia Pacific (Seoul)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
EU (Frankfurt)

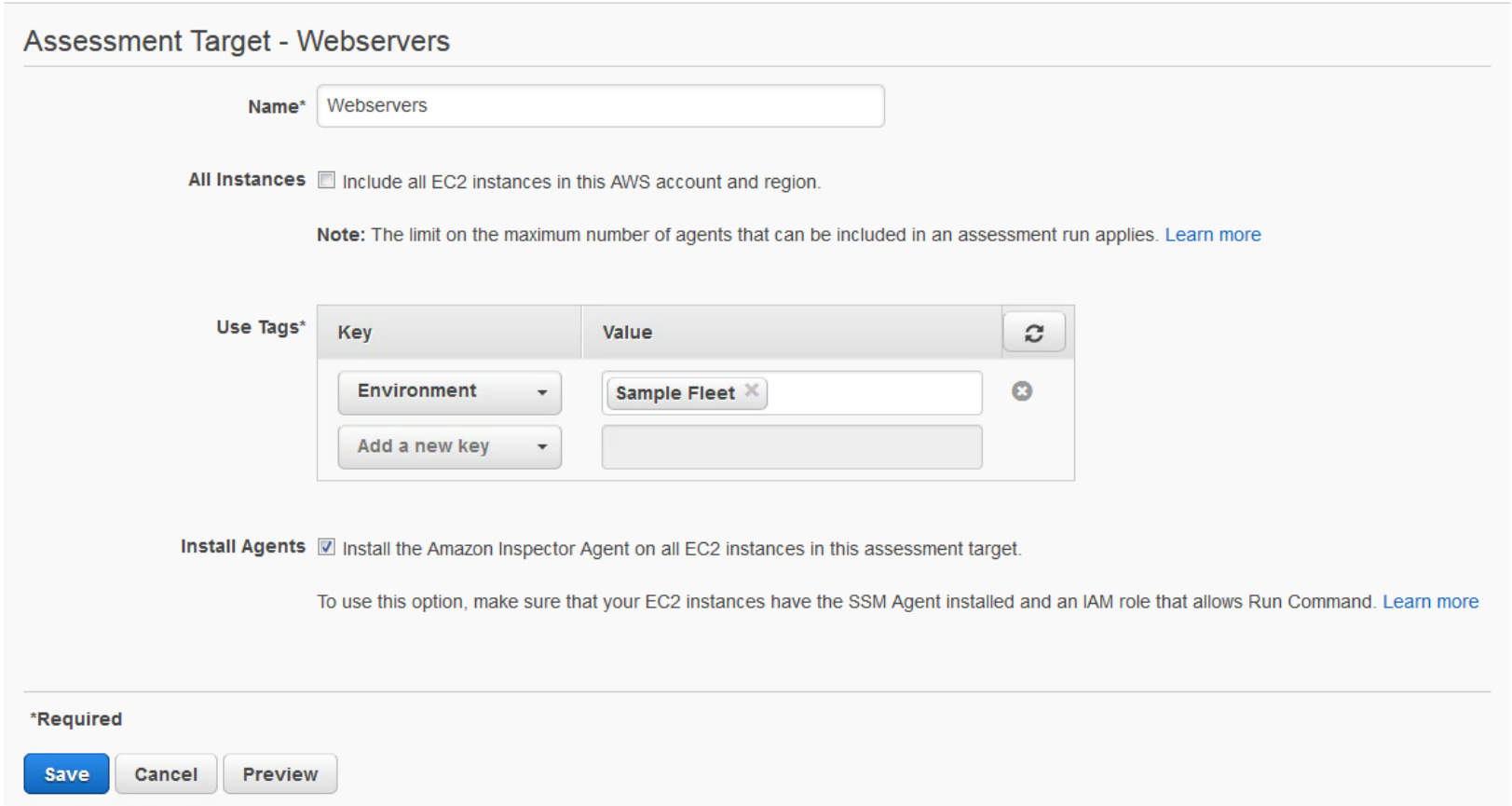
US East (Northern Virginia)
US East (Ohio)
US West (Northern California)
US West (Oregon)
EU (Ireland)

AWS GovCloud (US) - launched June 20th

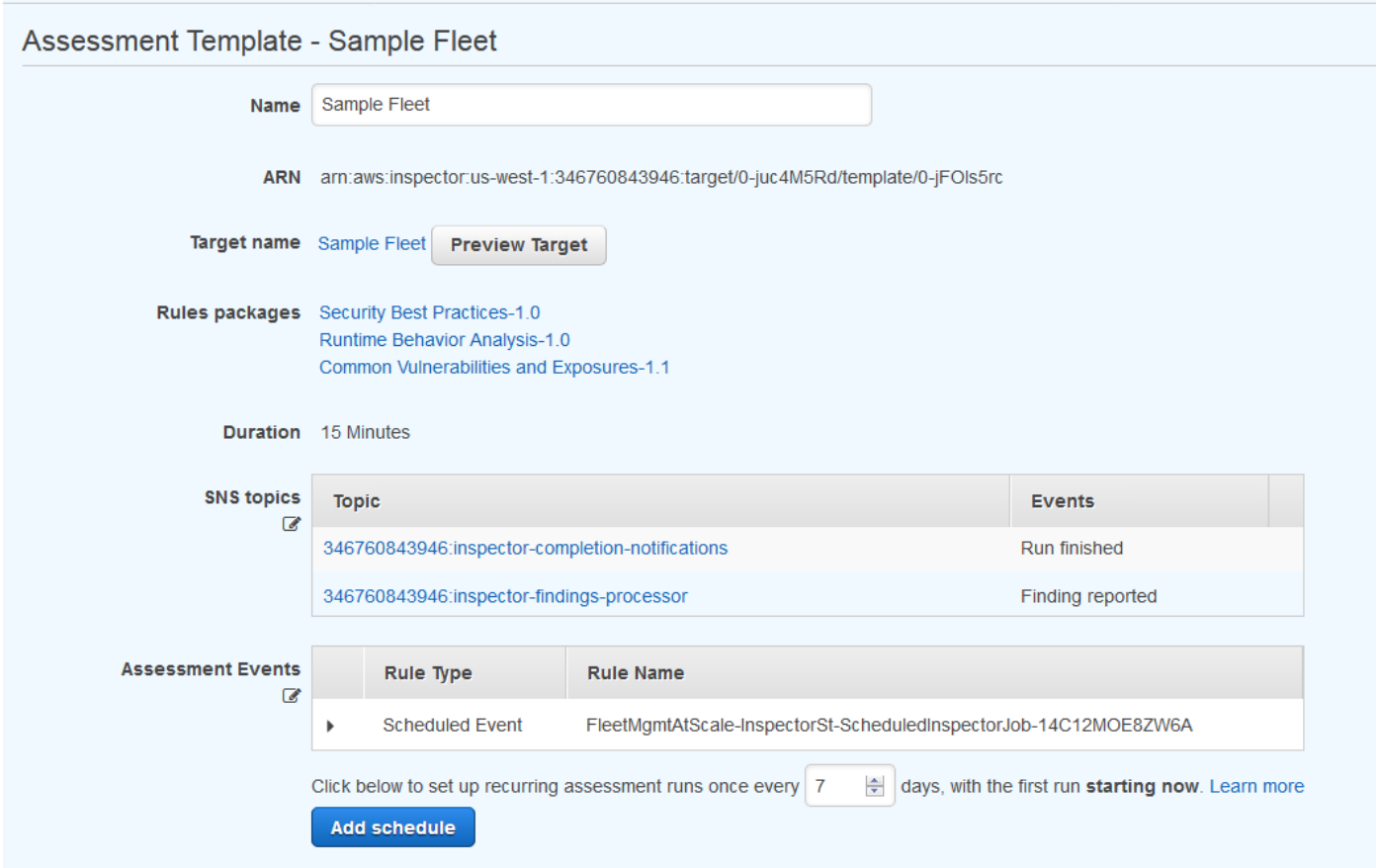
Learn more: https://aws.amazon.com/govcloud-us/getting-started/

Thank You!

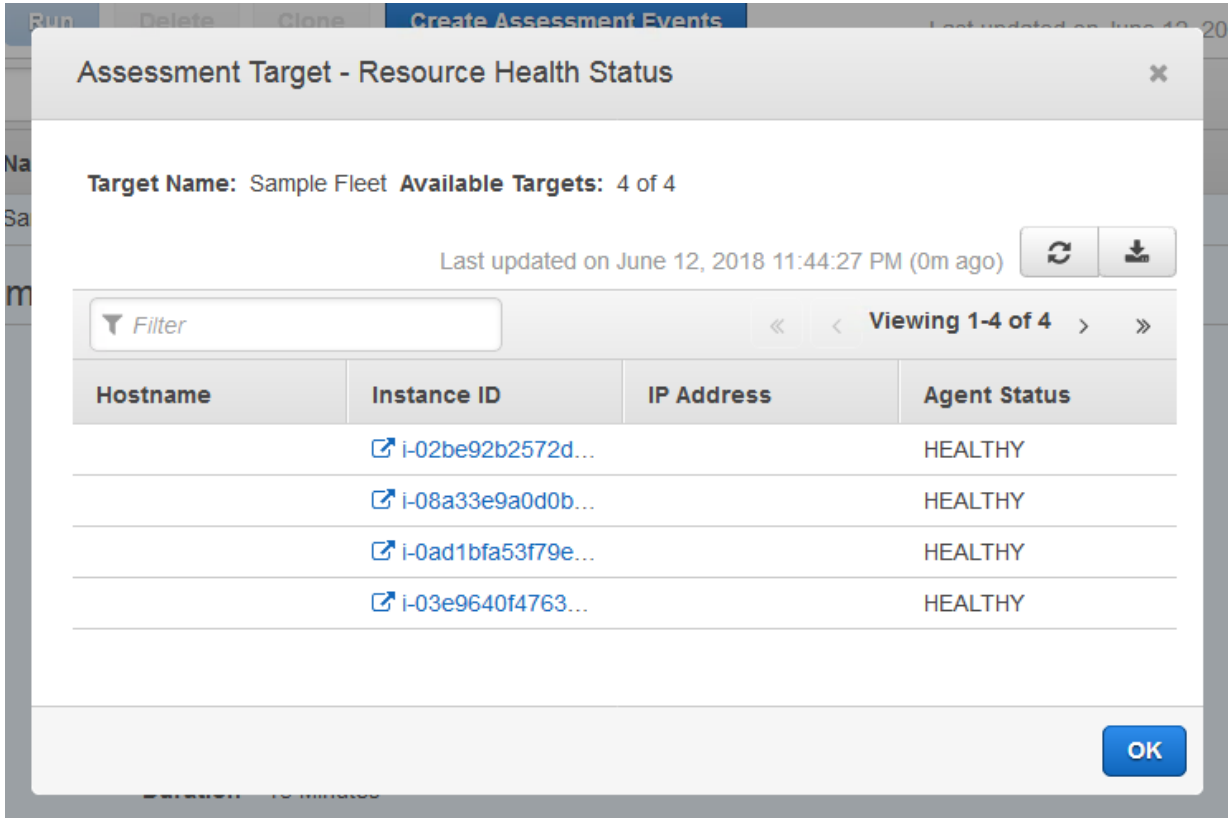
Assessment Target



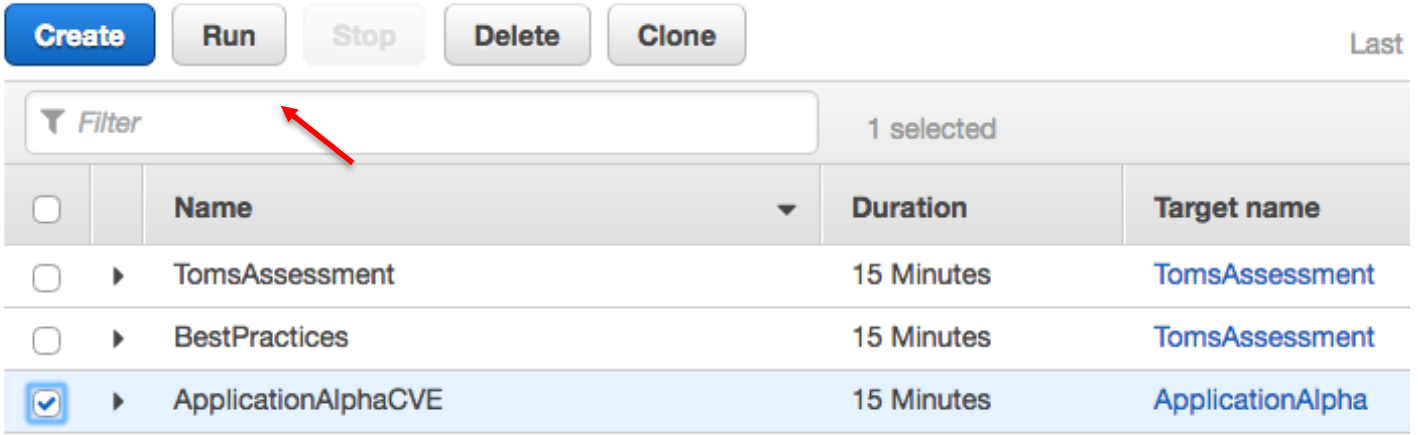
Assessment Template



Preview Target



Assessment Templates - Run



Assessment Runs

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment

Run | Cancel | Delete | Last updated

Filter | 1 selected

		Start time	Status	Template name	Findings
☑	▸	Today at 11:20 PM (G…	Analysis complete	InspectorToChime	225
☐	▸	Today at 10:50 PM (…	Analysis complete	Sample Fleet	233
☐	▸	Today at 10:22 PM (…	Analysis complete	Sample Fleet	233
☐	▸	Today at 9:43 PM (G…	Analysis complete	Sample Fleet	234
☐	▸	Today at 11:14 AM (G…	Analysis complete	Sample Fleet	233

Assessment Runs

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment

Run | Cancel | Delete | Last updated

Filter | 1 selected

		Start time	Status	Template name	Findings
☑	▸	Today at 11:20 PM (G…	Analysis complete	InspectorToChime	225
☐	▸	Today at 10:50 PM (…	Analysis complete	Sample Fleet	233
☐	▸	Today at 10:22 PM (…	Analysis complete	Sample Fleet	233
☐	▸	Today at 9:43 PM (G…	Analysis complete	Sample Fleet	234
☐	▸	Today at 11:14 AM (G…	Analysis complete	Sample Fleet	233

Customized Workflow

Instance i-03e9640f47634c6f7 is vulnerable to CVE-2018-0762

C

CuratedIns <no-reply@sns.amazonaws.com>

Dodge, Catherine

Wednesday, June 13, 2018 at 12:30 AM

Show Details

Title:
Instance i-03e9640f47634c6f7 is vulnerable to CVE-2018-0762

Description:
Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

Recommendation:
Use your Operating System's update feature to update package (see the CVE details). For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0762