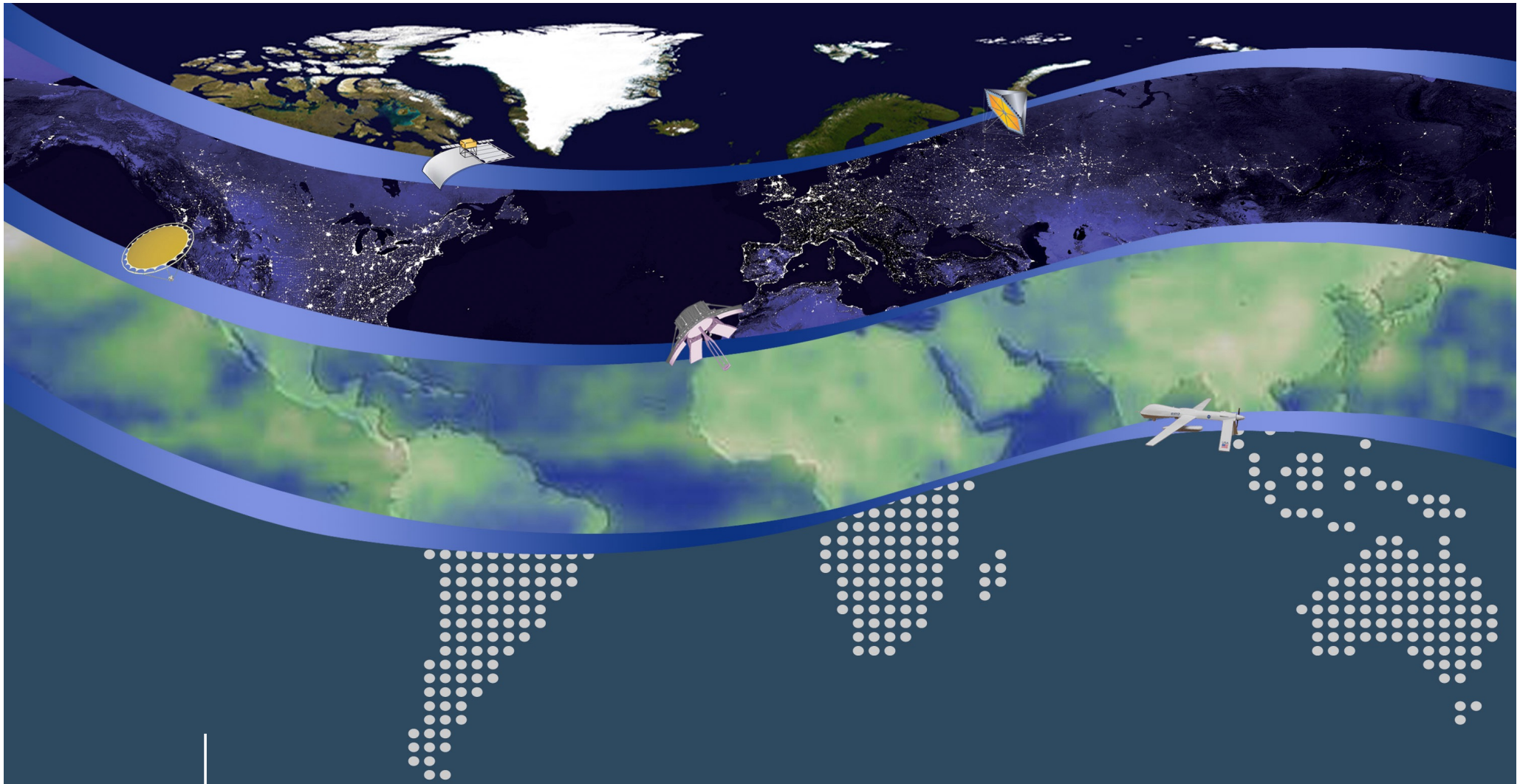


Annual Elevated Privileges Security Training Science Managed Cloud Environment (SMCE)

Last Updated: 13 June 2022

Computational and Information Sciences and Technology Office (CISTO)
GSFC Code 606

Topics

- Acronyms
- Continuous Vulnerability Scanning with AWS Inspector v2
- Remediation and Blocklist Processing
- Inspector v2 Reports
- AWS Inspector v2 Console Features
- Effective Vulnerability Management in SMCE
- Automated Patching using AWS Patch Manager

Acronyms

ACG	A Cloud Guru	IAM	Identity and Access Management
AMI	Amazon Machine Image	ISSO	Information Systems Security Officer
API	Application Programming Interface	ITAR	International Traffic in Arms Regulations
ATC	AWS Training and Certification	MFA	Multi-Factor Authentication
AWS	Amazon Web Services	NIST	National Institutes of Standards and Technology
CIS	Center for Internet Security	PI	Principal Investigator
CUI	Controlled Unclassified Information	RHEL	Red Hat Enterprise Linux
CVE	Common Vulnerabilities and Exposures	S3	Simple Storage Service
EC2	Elastic Compute Cloud	SLES	SUSE Linux Enterprise Server
ECR	Elastic Container Registry	SOC	Security Operations Center
FISMA	Federal Information Management Security Act	SSM	Systems Manager

User Agreements and Training Requirements

SMCE Agreement or Training Module	Who Should Take This	Time Frame
User Agreement	All console users	Annually
General Security Training	All console users	Annually
Elevated Privileges Security Training	Project SysAdmins, CloudAdmins	Annually

- Training is designed to help users understand current NASA security requirements and how they impact the operation of SMCE
- SMCE Users, PIs, and Project SysAdmins will need to work together with the ISSO and CloudAdmin Team to implement good security practices

Security is everyone's responsibility!

Shared Security Responsibility Model

Layer	SMCE CloudAdmins	Project SysAdmins
Application Layer	• Monitor application authentication for security compliance and provide recommendations for remediation	• Install/configure applications in a secure fashion • Create and update passwords to meet NASA guidelines
Container Layer	• Implement AWS Elastic Container Registry (ECR) for storage of approved Containers	• Store approved Containers in AWS Elastic Container Registry (ECR) • Update Containers to resolve vulnerabilities shown in Inspector v2
O/S Layer	• Monitor EC2 instances for security compliance and provide notifications for required patches	• Use SMCE supplied AMIs • Read and understand vulnerabilities from weekly Inspector v2 reports • Configure secure EC2 instances and implement patches as required
Cloud Layer	• Maintain Custom AMIs, and Monitor Password / API key age compliance	• Coordinate with the ISSO to ensure User Agreement is signed create IAM users
Physical Layer	• AWS provides secure facilities, hardware, and other capabilities	

Roles and Responsibilities

SMCE Team

SMCE Management

Project vetting, SMCE funding and financials, operational oversight

SMCE Cloud Administrators

Cloud-layer administration, cloud operations, secure images, setup projects, cloud accounts, security scans, security compliance, etc.

SMCE Cloud Architects

Cloud-layer operational solutions, SMCE services, prototyping, consulting, some training, and more

Project Teams

Project End Users/Service Users

Users of the project's services (NO console access), as defined by the PI, must adhere to the project and/or service requirements

Project Principal Investigator

Responsible for all aspects of the project, including funding, defining the project system administrators, ensuring security requirements are met

Project System Administrators

Defined by the PI, operating system administration, must respond to SMCE Elevated Privileges Security Training

Project Console Users

Defined by the PI, access to AWS console, must adhere to SMCE User Agreement and General Security Training

SMCE Users

Any user of the SMCE, to include Project End/Service Users, PIs, Project SysAdmins, and Project Console Users

SMCE Information Systems Security Officer

Maintain and implement security plan, cloud security operations, conduct training, maintain authorization to operate

Continuous Vulnerability Scanning in SMCE

- The SMCE leverages the continuous scanning model being employed by AWS Inspector v2 to identify vulnerabilities related to the NIST Common Vulnerability Enumeration (CVE) specifications

- Vulnerabilities in Inspector v2 are stored in an AWS repository that is updated continuously based on the following events:
  - EC2 instance new package installation
  - EC2 instance package update
  - EC2 instance start or restart
  - EC2 instance stop
  - CVE update/release (by NIST)
  - CIS Benchmark updates

- The SMCE DevOps team will produce a weekly custom report showing vulnerabilities for each EC2 instance using the Inspector v2 repository

Vulnerability Remediation

- SMCE PIs and Project SysAdmins will receive notifications each Saturday to include a link to a custom report showing vulnerabilities for each EC2 instance

- Project SysAdmins are responsible for remediating all vulnerabilities within the following timeframes:
  - Expedited (SOC MAR): 7 Calendar Days
  - Critical: 15 calendar days
  - High: 30 calendar days
  - Medium: 30 calendar days
  - Low: 60 calendar days

- Systems not patched within the above timeframes will be subject to their EC2 instances being temporarily shut down

- Project SysAdmins will need to use the Inspector v2 console and collaborate with the SMCE Security Team to ensure patches are applied in a timely manner

Blocklist Processing

- EC2 instances that have not been patched within the recommended timeframe will be placed on a “Blocklist”
- PIs and Project SysAdmins will be notified at least 7 days in advance of a pending action to place this instance on a Blocklist
- If the required actions to remediate the vulnerabilities are not completed within the number days specified for each level (Expedited, Critical, High, Medium, Low), the EC2 instance will be temporarily shut down, with all access blocked
- The SMCE ISSO and SMCE CloudAdmin team will distribute the Inspector v2 reports weekly to provide advance warning of pending blocklist actions

SMCE Weekly Inspector v2 Reports

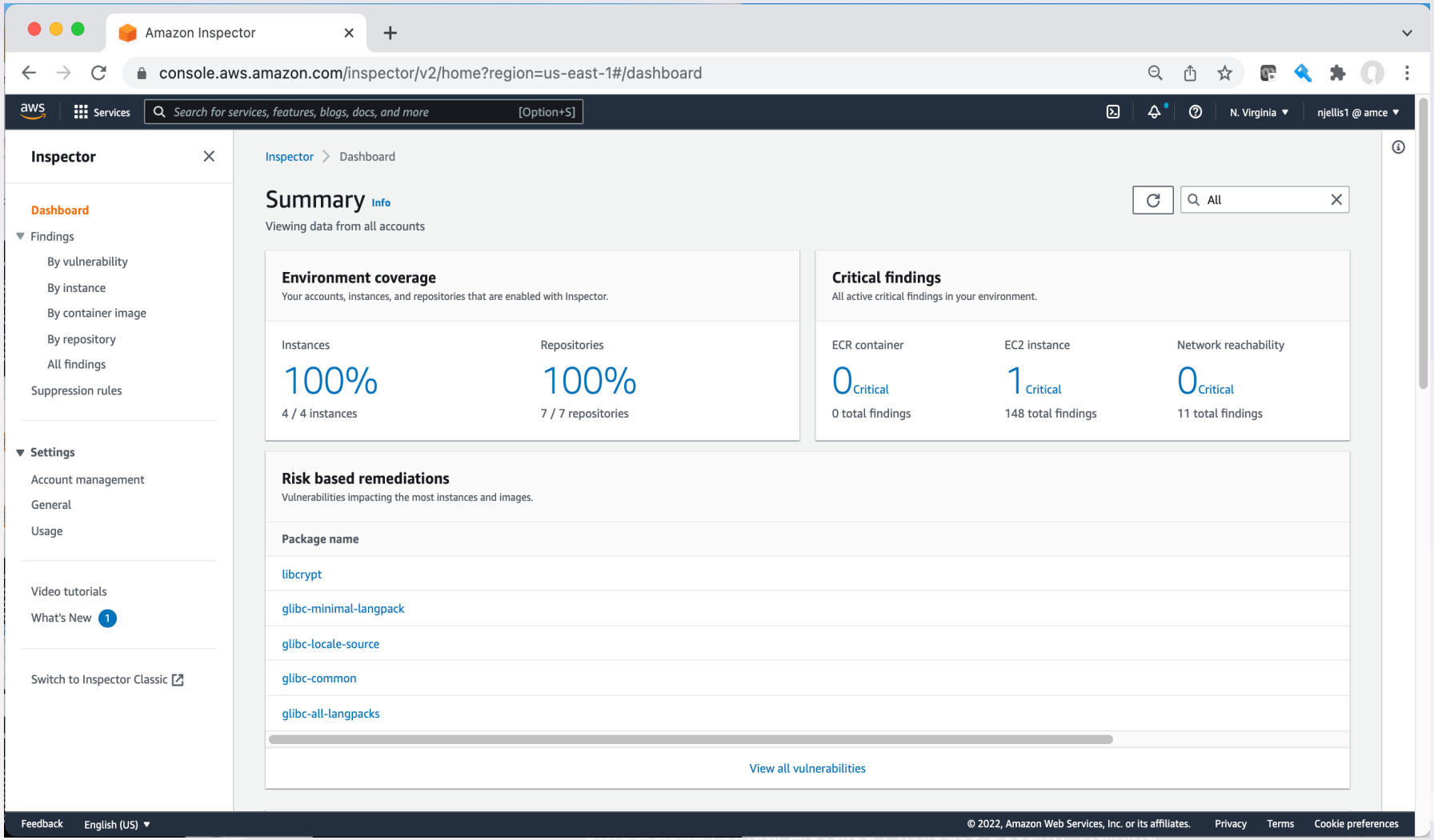
- Custom weekly vulnerability reports have been updated to support Inspector v2
- The reports are based on the continuously updated database of vulnerability information maintained by AWS
- Changed Fields:
  - **CVEs** – Contains more information about the vulnerability (not just the CVE #)
  - **Highest_Sev_First_Observed_Date** – Date when highest severity CVE was detected
  - **Highest_Severity** – The NIST rating of the highest-rated CVE for this instance
  - **Age_of_Oldest_and_Highest_Severity** – Age in days of highest rated and oldest CVE

InstanceId	Account	Region	CVEs	Highest_Sev_First_Observed_Date	Highest_Severity	Age_of_Oldest_and_Highest_Severity	Days Until Shutdown
i-000011122	smce-xxx	us-east-1	CVE-2021-44731 - snapd, CVE-2022-22827 – libexpat1-dev	1/8/22	HIGH	4	22
i-111122233	smce-yyy	us-east-1	CVE-2022-26385 - firefox	1/8/22	HIGH	4	21
i-111122244	smce-zzz	us-east-1	CVE-2020-26401 - kernel	1/8/22	MEDIUM	4	21
i-222333444	smce-aaa	us-east-1	CVE-2021-3997 – system-timesync	12/18/21	HIGH	25	Shutdown

Using the new SMCE Security Reports with Inspector v2

- Displays vulnerabilities for all active EC2 instances with SSM agent in a given region
- Allows for use of “Suppression Rules” to hide CVEs that have been risk-accepted
- Includes vulnerabilities for Elastic Container Registry (ECR) images
- Highlights Critical findings across multiple attack vectors, to include risks related to network availability/reachability
- Inspector v2 dashboard/console provides an enhanced interface to provide streamlined vulnerability management capabilities:
  - Facilitates drill-down to determine specific CVE information
  - Allows for use of “Suppression Rules” to hide CVEs that have been risk-accepted
  - Shows updated compliance information (within 15 minutes) to allow quick turn-around for remediation efforts

AWS Inspector v2: Dashboard



AWS Inspector v2: Instance Summary

Amazon Inspector

us-east-1.console.aws.amazon.com/inspector/v2/home?region=us-east-1#/settings/account-management/instances

NASA KBR

aws Services Search for services, features, blogs, docs, and more [Option+S] N. Virginia nost | 729474902545

S3

Inspector

- Dashboard
- Findings
  - By vulnerability
  - By instance
  - By container image
  - By repository
  - All findings
- Suppression rules
- **Settings**
  - Account management
  - General
  - Usage
- Video tutorials
- What's New
- Switch to Inspector Classic

Inspector > Settings > Account management > Instances

Account management Info

Manage your accounts, and review the coverage of your instances, repositories, and images.

Accounts | Instances | Repositories | Images

All	Scanning	Not scanning
4	3	1

Instances (4) Info

Resource type *EQUALS* AWS EC2 Instance *Add filter*

1

EC2 instance	EC2 instance name	Account	AMI	Operating system	Status
i-01dfa2b31e379dc7e	Solace PubSub+	729474902545	ami-05fd2acca90b8f479	LINUX	Scanning
i-05d5a7fd5f26be7c8	NOS-T Manager	729474902545	ami-0987d93a0ed9d9ab5	LINUX	Scanning
i-0774ab8ceb998becb	nost-nwis	729474902545	ami-0991e726bfcbce660	LINUX	Scanning
i-07abf57062b969978	NOS-T-Soil	729474902545	ami-0fc134bc23581882a	LINUX	Unmanaged Ec2 instance

Feedback

 Privacy Terms Cookie preferences

AWS Inspector v2: CVEs/Findings by Instance

Amazon Inspector

us-east-1.console.aws.amazon.com/inspector/v2/home?region=us-east-1#/findings/instances/i-01dfa2b31e379dc7e

NASA KBR

aws Services Search for services, features, blogs, docs, and more [Option+S] N. Virginia nost | 729474902545

S3

Inspector

- Dashboard
- Findings
  - By vulnerability
  - By instance
  - By container image
  - By repository
  - All findings
- Suppression rules

- Settings
  - Account management
  - General
  - Usage

- Video tutorials
- What's New

Switch to Inspector Classic

Details

EC2 instance	Creation date	Created by
i-01dfa2b31e379dc7e	October 26, 2020 6:04 PM (UTC-04:00)	729474902545
Role	**AWS account**	**Security group**
arn:aws:iam::729474902545:instance-profile/SMCE_SSMAgent	729474902545	nost-broker
Amazon machine image		
ami-05fd2acca90b8f479		

Finding summary

Package findings

7 Critical 15 High 8 Medium

Findings (38)

Choose a row to view the finding details. All findings are related to this instance.

Active | Resource ID EQUALS i-01dfa2b31e379dc7e | Add filter

1 2

Severity	Title	Impacted resource	Type	Age	Status
Critical	CVE-2022-23852 - expat	i-01dfa2b31e379dc7e	Package Vulnerability	20 days	Active
Critical	CVE-2022-22823 - expat	i-01dfa2b31e379dc7e	Package Vulnerability	20 days	Active
Critical	CVE-2022-22824 - expat	i-01dfa2b31e379dc7e	Package Vulnerability	20 days	Active

Feedback © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Inspector v2: Findings/CVE Drilldown

Amazon Inspector

us-east-1.console.aws.amazon.com/inspector/v2/home?region=us-east-1#/findings/instances/i-01dfa2b31e379dc7e

NASA KBR

aws Services Search for services, features, blogs, docs, and more [Option+S] N. Virginia nost | 729474902545

S3

Inspector

- Dashboard
- Findings
  - By vulnerability
  - By instance
  - By container image
  - By repository
  - All findings
- Suppression rules
- **Settings**
  - Account management
  - General
  - Usage
- Video tutorials
- What's New
- Switch to Inspector Classic

-profile/SMCE_SSMAgent 729474902545

Amazon machine image
ami-05fd2acca90b8f479

Created by
729474902545

Security group
nost-broker

Finding summary
Package findings
7 Critical 15 High
8 Medium

Findings (38)
Choose a row to view the finding details. All findings are related to this instance.

Active | Resource ID *EQUALS* i-01dfa2b31e379dc7e

1 2

Severity	Title	Impacted resource
Critical	CVE-2022-23852 - expat	i-01dfa2b31e379dc7e
Critical	CVE-2022-22823 - expat	i-01dfa2b31e379dc7e
Critical	CVE-2022-22824 - expat	i-01dfa2b31e379dc7e
Critical	CVE-2022-25235 - expat	i-01dfa2b31e379dc7e

CVE-2022-23852 - expat
Finding ID: arn:aws:inspector2:us-east-1:729474902545:finding/1e888b61001028bc34802a11892f7dd2

expat (libexpat) is susceptible to a software flaw that causes process interruption. When processing a large number of prefixed XML attributes on a single tag can libexpat can terminate unexpectedly due to integer overflow. The highest threat from this vulnerability is to availability, confidentiality and integrity.

Finding details | Inspector Score

Finding overview	
AWS account ID	729474902545
Severity	Critical
Type	Package Vulnerability
Last seen	April 5, 2022 6:44 PM (UTC-04:00)
Created at	April 5, 2022 6:44 PM (UTC-04:00)
Affected packages	
Name	expat
Version	0:2.1.0-12.el7.X86_64
Package manager	OS
Vulnerability details	
Vulnerability ID	CVE-2022-23852

Feedback © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Automated Patching for SMCE Systems – How?

- Can be implemented via AWS Patch Manager
  - Part of AWS Systems Manager within the Node Management group
  - Requires Systems Manager agent on each EC2 instance to be present

- Facilitates automated patch activities
  - For one or more EC2 instances, or
  - For an established Patch Group

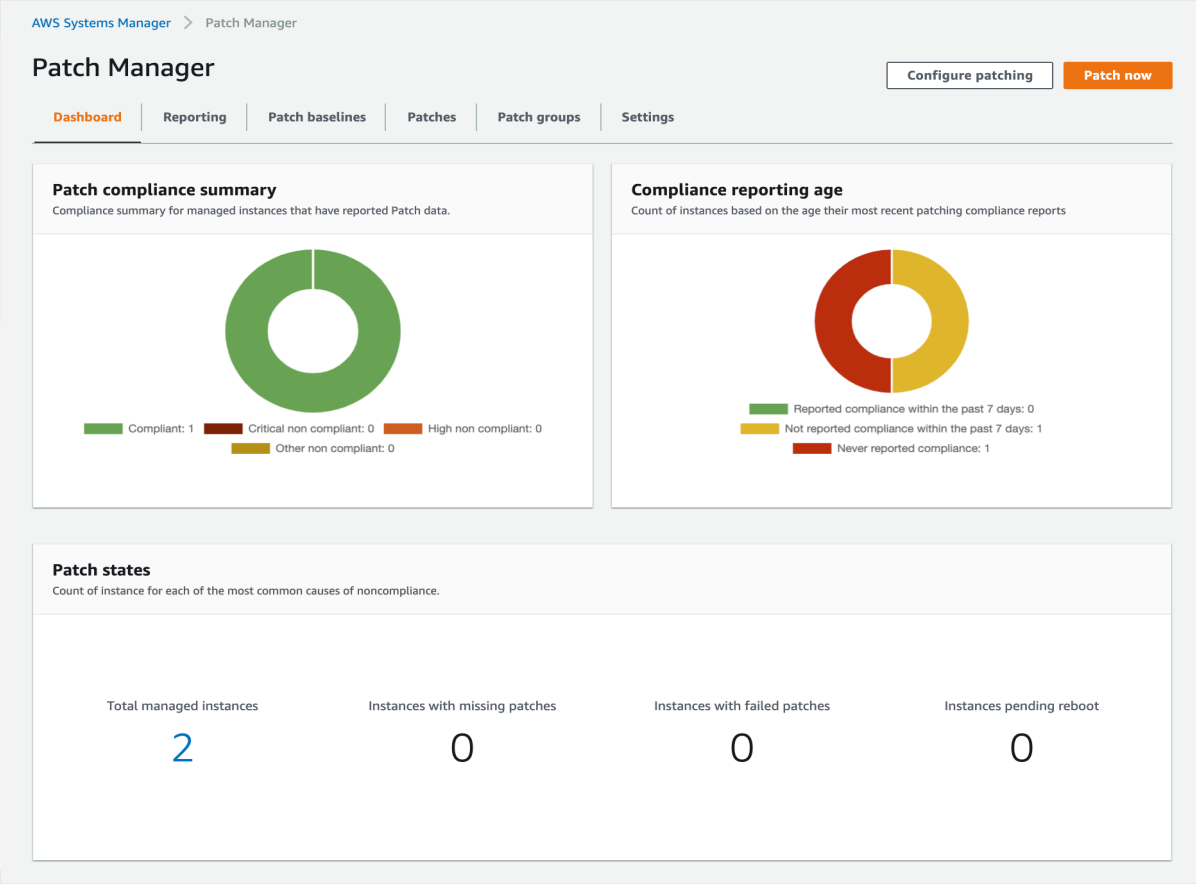
Automated Patching for SMCE Systems – When?

- ***You Decide!***
  - Patch Manager allows for the creation of a Maintenance Window at your discretion
  - Maintenance Windows establish a repetitive schedule when required patches will be deployed
  - Patch Manager includes option to use cron for schedule management

- Note: Notifications of Users prior to automated patching is recommended
  - Reboot of one or more EC2 instance may occur if system-level packages are included with list of deployed patches

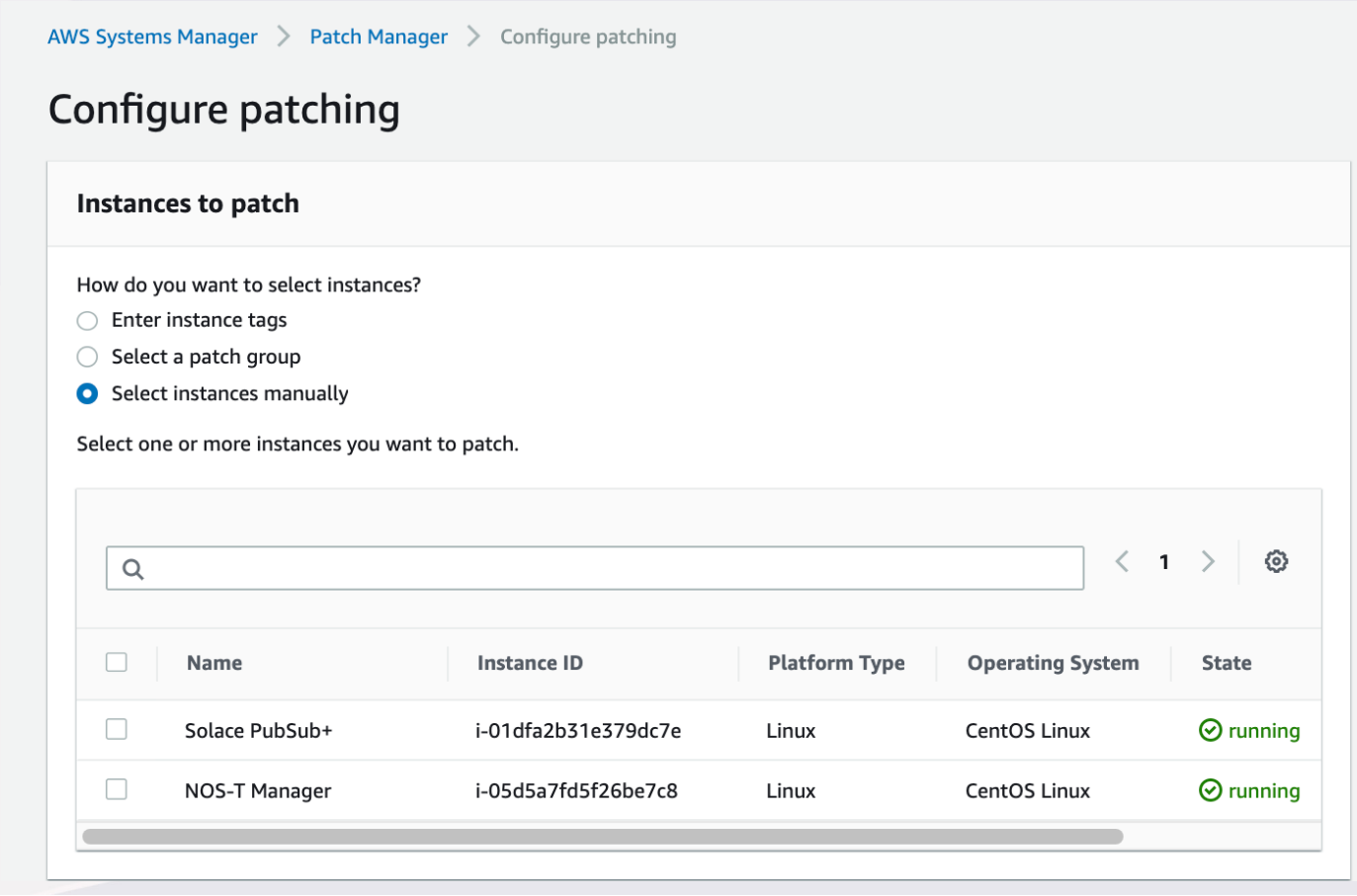
AWS Patch Manager – Dashboard / Starting Point

- Patch Manager dashboard provides a summary of all instances that are currently managed (with an active SSM agent)



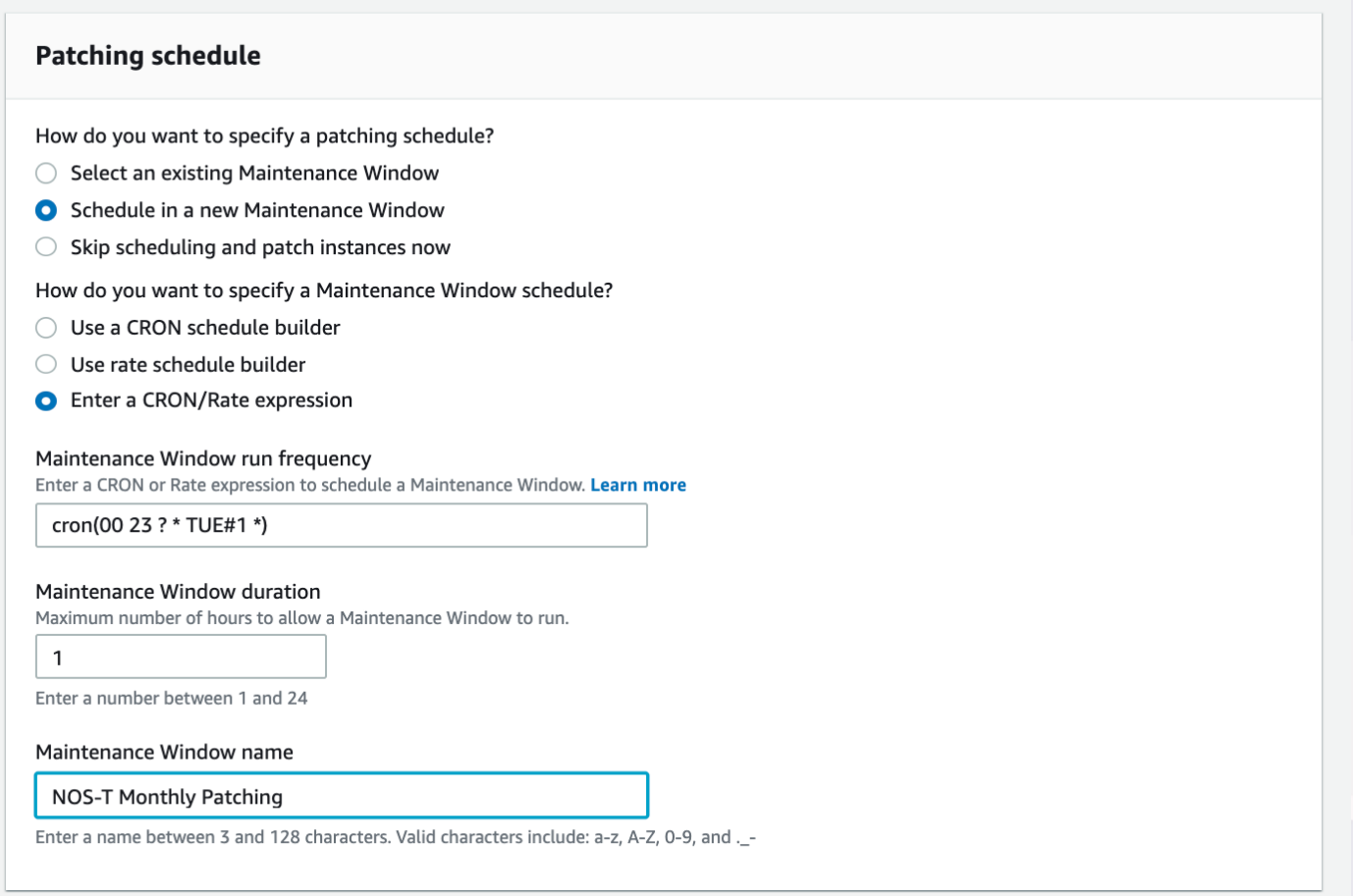
AWS Patch Manager – Configure Patching / Select Instances

- Allows for selection of one or more EC2 instances to be part of a patch group



Patching Schedule / Maintenance Window / Cron

- Allows the project sysadmin to specify a patch maintenance window using standard cron expressions



Patching Operation / Results

- Allows for automatic/unintended installation of all approved patches
- Note: Kernel-level patches will require a manual reboot

Patching operation

- (●) **Scan and install**
  Scans each target instance and compares its installed patches with the list of approved patches in the patch baseline. Downloads and installs all approved patches that are missing from the instance.
- ( ) **Scan only**
  Scans each target instance and generates a list of missing patches for you to review.

▼ Additional settings

If any instance you selected belongs to a patch group, Patch Manager patches your instances using the registered patch baseline of that patch group. If an instance is not configured to use a patch group, Patch Manager uses the default patch baseline for the operating system type of the instance.

Patching History and Recurring Tasks

- Allows for viewing of past and future patching activities

Patch operations history

This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

Filter tasks

1

Patch operation	Started by	Document name	End time	Status	Targets
Install	Other	AWS-RunPatchBaseline	June 1, 2021, 7:00 PM EDT	Success	InstanceIds: i-01dfa2b31e379dc7e

Recurring patching tasks

The following is a list of State Manager associations and maintenance windows that run any patching-related task. Choose a task name to view its details

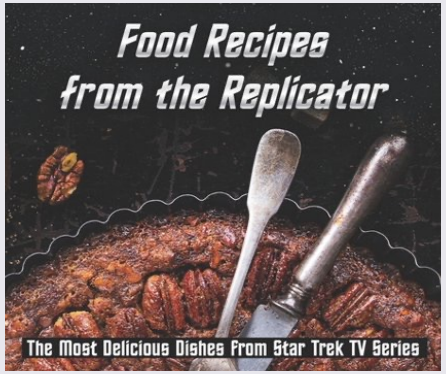
1

Patching task name	Task type	Document name	Schedule
PatchingTask	MW Task	AWS-RunPatchBaseline	cron(00 23 ? * TUE#1 *)

Automated Patching - Summary

- Use AWS Patch Manager with established maintenance windows
- Leverage cron-like capabilities for schedule management
- To avoid business impact, notify users prior to automated patching activities
- Backup instances prior to automated patch deployment to provide rollback capability if needed
- Perform manual reboots of affected EC2 instances if kernel-level patches are applied

Recipe for Effective Vulnerability Management in SMCE



- Download and review the Inspector reports sent to you each Saturday
- Respond to emails from the SMCE security team to provide feedback about patching status and “un-patchable” CVEs
- Use the Inspector v2 console to gather the information necessary and complete updates necessary to avoid having your instances marked as “Shutdown”
- Use the tools/methods you are most familiar with to implement patches
  - AWS Patch Manager
  - yum update
- Please contact the SMCE Security or SMCE CloudAdmin team at support@nccs.nasa.gov if you need assistance!

Recommended Cloud Training and Certifications for SMCE Project System Administrators

- Cloud Training Resources
  - A Cloud Guru (ACG) - https://acloud.guru
  - AWS Training and Certification (ATC) – https://www.aws.training
- Courses
  - (ACG) Introduction to AWS (5.5 hours)
  - (ATC) AWS Skills Center: Cloud Practitioner Essentials - Parts 1 & 2 (4 Hours)
  - (ACG) AWS Certified Cloud Practitioner (16 hours)
  - (ATC) Developing Serverless Solutions on AWS (3 Days)
- Certifications / Learning Paths
  - AWS Certified Cloud Practitioner
  - AWS Certified Solutions Architect
  - AWS Certified Security – Specialty
  - AWS Certified SysOps Administrator
  - AWS Certified DevOps Engineer