Integrating security testing into your container build pipeline

Laurent Domb Principal Solutions Architect AWS

Goals

- Learn about container security using DevSecOps
- Learn about open-source container security tools and standards
- Learn about AWS development tools and DevOps services



Why is container security different?

Virtual machines

Cats application	Dogs application					
Bins/libs	Bins/libs					
Guest OS	Guest OS					
Hypervisor						
Host OS						
Server						







Containers on AWS





AWS shared responsibility model



Amazon ECS: AWS shared responsibility model

AWS Fargate: AWS shared responsibility model

Automated pipelines: DevSecOps

Speaking of automation, you should automate everything, including

- Code and container builds
- Infrastructure via infrastructure as code patterns
- Deployments
- Process of making things self-healing
- Security!

Make it fast and easy for your team to do the right thing!

- Host security
- Image security
- Denial of service
- Credentials and secrets
- Container breakouts
- Runtime security

- Host security
- Image security
- Denial of service
- Credentials and secrets
- Container breakouts
- Runtime security

- Host security
- Image security
- Denial of service
- Credentials and secrets
- Container breakouts
- Runtime security

Full blown OS or Container Optimized

ECS-optimized AMI

Debian/SuSe/RHEL

CoreOS

- Host security
- Image security
- Denial of service
- Credentials and secrets
- Container breakouts
- Runtime security

Security best practices for container images

- Less is more (secure)
- No secrets in them
- One service per container
- Minimize container footprint
- Include only what is needed at runtime

Security best practices for container images

- Use known and trusted base images
- Scan the image for CVEs
- Specify USER in Dockerfile (otherwise it's a root)
- Use unique and informative image tags

Image security

- Docker linting: Validation of Docker configuration (PCI DSS v3.2.1 Req 2.2)
 - hadolint
 - dockerfile_lint
- Secrets scanning in images (PCI DSS v3.2.1 Req 6.3.1)
 - truffleHog
 - git-secrets
- Vulnerability scanning of images in your build pipeline (PCI DSS v3.2.1 Req 6.1)
 - Anchore Open-Source Engine
 - CoreOS Clair
 - Amazon ECR

Image Scanning in AWS

\leftrightarrow \rightarrow C $($ console.aws.am	azon.com/e	cr/repositories/cdk/workshopmgmtnukec	lusterworkshopmgmtnukercontainerimagefa2b8535/?	region=us-east-1					Q	. 🕁 👂 🖪 🥺 🛛) i
Apps 🚯 AWS Wisdom Fina	aws 🔇	Contact seller								🗎 Other Boo	kmarks
aws Services - F	Resource Gr	oups 🗸 🛠						û Admin/Ido-I	isengard @ domb 👻	N. Virginia 👻 Support	
Amazon Container ×	⊘ Scan s	started on the selected image									X
Services	ECR	> Repositories > cdk/workshopmgmtnukec	lusterworkshopmgmtnukercontainerimagefa2b8535								
Amazon ECS Clusters	cdk	<pre></pre>	usterworkshopmgmtnukercont	ainerimagefa2b8535						View push commands	,
Task definitions		(4)									7
Amazon EKS	Im	hages (1)		7					G	Delete Scan	
Clusters		, rinu iniuges									_
Amazon ECD		Image tag	Image URI			Pushed at 🔹 🔻	Digest	Size (MB) ⊽	Scan status	Vulnerabilities	
Repositories		latest	141298987014.dkr.ecr.us-east-1.amazonaws.com/ci	dk/workshopmgmtnukeclusterworkshopmgmtnukercontainerimagefa2b8	8535:latest	09/27/19, 09:53:47 AM	🗇 sha256:49e268d56	247.42	In progress		
Images											
Permissions											
Lifecycle Policy											
Tags											

aws

Image Scanning in AWS

aws Services - Re	esource Groups 🗸 🕻				Ĺ Admi	in/ldo-Isengard @ d	omb 👻 N. Virginia 💌 Support 👻	
Amazon Container ×	⊘ Scan started on the selected image							×
Amazon ECS Clusters Task definitions	ECR > Repositories > cdk/workshopmgmtnukeclu	sterworkshopmgmtnukercontainerimagefa2b8535 Isterworkshopmgmtnukercontainerimagefa2b8535					View push commands	
Amazon EKS Clusters	Images (1) Q. Find images						C Delete Scan < 1 > ©	
Amazon ECR Repositories Images	Image tag Iatest	Image UKI	Pushed at •	Digest	Size (MB) ♥ 247.42	Complete	Vutnerabilities	
Permissions Lifecycle Policy Tags								

Image Scanning in AWS

\leftrightarrow \rightarrow C \cong console.aws.ama	zon.com/ecr/repositories/cdk	/workshopmgmtnukeclu	sterworkshopmg	ntnukercontainerimagefa2b8535/image/sha256:49e268d56	61ed9f537e436f26e23a9bd6ddb1fcd698f20e	9ebeaa13883df1b1c/scan-results?region=us-east-1	९ 🖈 💩 🖪 🐸 🕕 🗄
👯 Apps 🕑 AWS Wisdom Fina 🗎	AWS 🚷 Contact seller						Cther Bookmarks
aws Services - Re	source Groups 🗸 🔸						⚠ Admin/Ido-Isengard @ domb × N. Virginia × Support ×
Amazon Container $ imes$ Services	ECR > Repositories >	cdk/workshopmgmtnukeclu	sterworkshopmgmt	nukercontainerimagefa2b8535 > sha256:49e268d5661ed9f537e4	36f26e23a9bd6ddb1fcd698f20e9ebeaa13883df1b1c		
Amazon ECS	Overview						
Clusters Task definitions							
	Critical		High	Medium	Low	Informational	Undefined
Amazon EKS Clusters	0		4	75	80	14	0
Amazon ECR	Vulnerabilities (17	3)					
Repositories	Q Find vulnerabilities						< 1 2 >
Permissions	Name \bigtriangledown	Package ∇	Severity v	Description			
Lifecycle Policy	CVE-2018-0501 🗹	apt:1.6.3	HIGH	The mirror:// method implementation in Advanced Package Tool (APT) 1.6.x before 1.6.4 and 1.7.x before 1.7.0~alpha3 n	mishandles gpg signature verification for the InRelease file of a fal	lback mirror, aka mirrorfail.
Tays	CVE-2019-3462 🔀	apt:1.6.3	HIGH	Incorrect sanitation of the 302 redirect field in HTTP transport met	hod of apt versions 1.4.8 and earlier can lead to conter	nt injection by a MITM attacker, potentially leading to remote cod	e execution on the target machine.
	CVE-2018-16865 🖸	systemd:237- 3ubuntu10.3	HIGH	An allocation of memory without limits, that could result in the sta this flaw to crash systemd-journald or execute code with journald p	ck clashing with another memory region, was discoven privileges. Versions through v240 are vulnerable.	red in systemd-journald when many entries are sent to the journal	socket. A local attacker, or a remote one if systemd-journal-remote is used, may use
	CVE-2018-16864 🖸	systemd:237- 3ubuntu10.3	HIGH	An allocation of memory without limits, that could result in the sta or escalate his privileges. Versions through v240 are vulnerable.	ck clashing with another memory region, was discoven	red in systemd-journald when a program with long command line	arguments calls syslog. A local attacker may use this flaw to crash systemd-journald
	CVE-2016-1585 🔀	apparmor:2.12- 4ubuntu5.1	MEDIUM	In all versions of AppArmor mount rules are accidentally widened v	when compiled.		
	CVE-2019-14444 🔀	binutils:2.30- 21ubuntu1~18.04.1	MEDIUM	apply_relocations in readelf.c in GNU Binutils 2.32 contains an inte	ger overflow that allows attackers to trigger a write acc	cess violation (in byte_put_little_endian function in elfcomm.c) via	a an ELF file, as demonstrated by readelf.
	CVE-2019-12900 🗹	bzip2:1.0.6-8.1	MEDIUM	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an ou	t-of-bounds write when there are many selectors.		
	CVE-2018-16839 🖸	curl:7.58.0- 2ubuntu3.2	MEDIUM	Curl versions 7.33.0 through 7.61.1 are vulnerable to a buffer over	run in the SASL authentication code that may lead to d	Jenial of service.	
	CVE-2018-16890 🗹	curl:7.58.0- 2ubuntu3.2	MEDIUM	libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to a heap overflow vulnerability. Using that overflow, a malicious or broken f	b buffer out-of-bounds read. The function handling inco iTLM server could trick libcuri to accept a bad length +	coming NTLM type-2 messages (`lib/vauth/ntlm.cntlm_decode_ty - offset combination that would lead to a buffer read out-of-bound	ype2_target`) does not validate incoming data correctly and is subject to an integer ds.
	CVE-2019-5481 🔀	curl:7.58.0- 2ubuntu3.2	MEDIUM	Double-free vulnerability in the FTP-kerberos code in cURL 7.52.0	to 7.65.3.		
	CVE-2019-5482 🔀	curl:7.58.0- 2ubuntu3.2	MEDIUM	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4	to 7.65.3.		
	CVE-2019-5436 🖸	curl:7.58.0- 2ubuntu3.2	MEDIUM	A heap buffer overflow in the TFTP receiving code allows for DoS of	r arbitrary code execution in libcurl versions 7.19.4 thr	rough 7.64.1.	
	CVE-2018-14618 🛂	curl:7.58.0- 2ubuntu3.2	MEDIUM	curl before version 7.61.1 is vulnerable to a buffer overrun in the N The length value is then subsequently used to iterate over the pass This integer overflow usually causes a very small buffer to actually	ITLM authentication code. The internal function Curl_ni word and generate output into the allocated storage b get allocated instead of the intended very huge one, n	ttlm_core_mk_nt_hash multiplies the length of the password by tw buffer. On systems with a 32 bit size_t, the math to calculate SUM making the use of that buffer end up in a heap buffer overflow. (The system is a state of the system is a state of the system is a state of the system is a system of the system is a system of the system	vo (SUM) to figure out how large temporary storage area to allocate from the heap. triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). is bug is almost identical to CVE-2017-8816.)
	CVE-2019-3822 🔀	curl:7.58.0- 2ubuntu3.2	MEDIUM	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a sta previously received data. The check that exists to prevent the local large 'nt response' data is extracted from a previous NTLMv2 head header.	rck-based buffer overflow. The function creating an out buffer from getting overflowed is implemented wrong er provided by the malicious or broken HTTP server. Sur provided by the malicious or broken HTTP server.	tgoing NTLM type-3 header (`lib/vauth/ntlm.cCurl_auth_create_ gly (using unsigned math) and as such it does not prevent the over ch a large value' needs to be around 1000 bytes or more. The act	ntlm_type3_message() '), generates the request HTTP header contents based on flow from happening. This output data can grow larger than the local buffer if very ual payload data copied to the target buffer comes from the NTLMv2 type-2 response
	CVE-2018-16842 🔀	curl:7.58.0- 2ubuntu3.2	MEDIUM	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based	buffer over-read in the tool_msgs.c:voutf() function th	hat may result in information exposure and denial of service.	
	CVE-2019-8457 🔀	db5.3:5.3.28- 13.1ubuntu1	MEDIUM	SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap or	ut-of-bound read in the rtreenode() function when han	dling invalid rtree tables.	
				dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13	12, as used in DBusServer in Canonical Upstart in Ubur	ntu 14.04 (and in some, less common, uses of dbus-daemon), allo	ws cookie spoofing because of symlink mishandling in the reference implementation

DevSecOps container pipeline

© 2019. Amazon Web Services. Inc. or its affiliates. All rights reserved.

- Host security
- Image security
- Denial of service
- Credentials and secrets
- Container breakouts
- Runtime security

Credentials and secrets

AWS has Parameter Store and AWS Secrets Manager to store your secrets

They are integrated into Amazon ECS, but you need to call them within the pod on Kubernetes via AWS CLI or SDK Assigning an IAM role to an instance, task, or function means that the right AWS access key and secret to call the AWS CLI or SDK are transparently obtained and rotated

Benefits of Using IAM Roles for Tasks

Credential Isolation: A container can only retrieve credentials for the IAM role that is defined in the task definition to which it belongs; a container never has access to credentials that are intended for another container that belongs to another task.

Authorization: Unauthorized containers cannot access IAM role credentials defined for other tasks.

Auditability: Access and event logging is available through CloudTrail to ensure retrospective auditing. Task credentials have a context of taskArn that is attached to the session, so CloudTrail logs show which task is using which role.

Pipeline high level overview

aws RE:INFORCE

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Thank you!

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.