



Banorte

Seguridad en Contenedores

Trend Micro



Risk Quantification & Evolution





Container Security



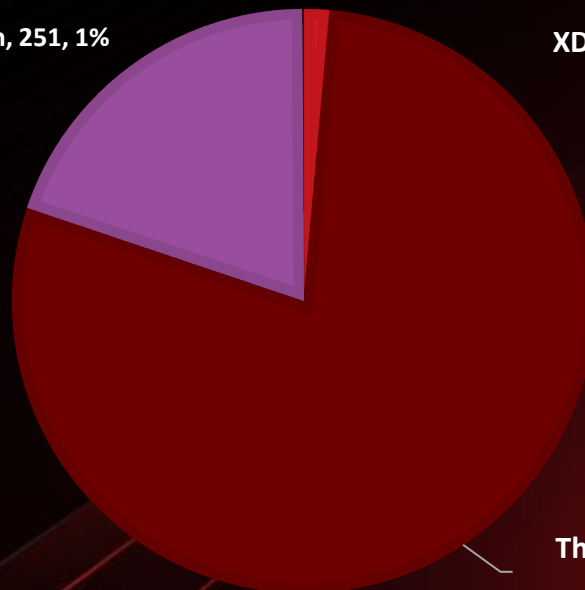
High Risk Container Cluster



System configuration, 251, 1%

XDR detection, 19, 0%

Vulnerabilities,
3490, 20%



- System configuration
- Threat detection
- Vulnerabilities
- XDR detection

Threat detection, 13939, 79%

Observed Attack Techniques

telemetry	Medium	Remote File Copy Tool in the Container	Command for external file transfer d...	TA0011	T1105
Highlighted objects	processCmd	curl -s http://172.30.11.94:8083/connectors/online-telemetry/status			
	parentCmd	sh -c /home/appuser/healthcheck.sh			
	ruleName	(T1105)Launch Ingress Remote File Copy Tools in Container			
	clusterName	Cluster_prueba_120824			
	k8sPodName	telemetry-5df7c9d8cc-gdxvf			
	containerName	telemetry			
	containerImage	icr.io/cpopen/turbonomic/kinesis-kafka-connect:8.12.5			
	k8sNamespace	turbonomic			



(T1105) Launch Ingress Remote File Copy Tools in Container

- La detección de la herramienta de copia de archivos remotos en el contenedor sugiere un comportamiento sospechoso que puede estar relacionado con la exfiltración de datos o el intento de establecer comunicaciones no autorizadas.
- La severidad media indica que el evento tiene un impacto potencial, pero puede no estar relacionado con un ataque directo. Sin embargo, es crucial investigarlo para evitar futuras explotaciones.

Mitigación

- Revisión de Logs: Analizar los logs de red y sistema para identificar patrones de comportamiento anómalos en el contenedor afectado.
- Restricciones de Red: Implementar restricciones de salida para contenedores, evitando que se comuniquen con endpoints no autorizados.
- Análisis de la Imagen: Realizar un escaneo de seguridad completo de la imagen icr.io/cpopen/turbonomic/kinesis-kafka-connect:8.12.5 para identificar vulnerabilidades conocidas o configuraciones inseguras.
- Implementar Controles de Integridad: Verificar la integridad del script healthcheck.sh y otros archivos críticos en el contenedor para detectar modificaciones no autorizadas.

Observed Attack Techniques

ms		Medium	Java Initiated Unix Shell Process in Container	Java executed unix shell in the contai...	TA0002	T1059.004
Highlighted objects	processCmd parentCmd clusterName k8sPodName	debug-options /opt/jboss/container/java/jvm/debug-options run-java.sh /opt/jboss/container/java/run/run-java.sh Cluster_prueba_120824 ap1023-portal-devsecops-frontend-dev-ms-854c458bfc-222xq				
ms		Medium	Java Initiated Unix Shell Process in Container	Java executed unix shell in the contai...	TA0002	T1059.004
Highlighted objects	processCmd parentCmd clusterName k8sPodName	java-default-op /opt/jboss/container/java/jvm/java-default-options run-java.sh /opt/jboss/container/java/run/run-java.sh Cluster_prueba_120824 ap1023-portal-devsecops-frontend-dev-ms-854c458bfc-222xq				

(T1059.004) Java Initiated Unix Shell Process in Container

- Este evento indica que un proceso Java en el contenedor ha iniciado un shell Unix, lo cual puede ser un comportamiento sospechoso si no está planeado o autorizado.
- Un atacante podría utilizar este shell para ejecutar comandos arbitrarios dentro del contenedor, comprometiendo su integridad y confidencialidad.
- El uso de shells en combinación con procesos Java puede permitir a un atacante establecer persistencia en el contenedor afectado.

Mitigación

- Verificar las configuraciones del contenedor y las opciones de inicio de Java para asegurar que no se permiten opciones de depuración o de ejecución de scripts de shell innecesarios.
- Implementar monitoreo continuo para detectar cualquier actividad anómala o no autorizada en los procesos de Java dentro de los contenedores.
- Asegurarse de que los contenedores se ejecuten con los permisos mínimos necesarios, evitando el uso de usuarios privilegiados o configuraciones permisivas.

Observed Attack Techniques

telemetry	Medium	Remote File Copy Tool in the Container	Command for external file transfer d...	TA0011	T1105
Highlighted objects	processCmd parentCmd ruleName clusterName k8sPodName containerName containerImage k8sNamespace	curl -s http://172.30.11.94:8083/connectors/online-telemetry/status sh -c /home/appuser/healthcheck.sh (T1105)Launch Ingress Remote File Copy Tools in Container Cluster_prueba_120824 telemetry-5df7c9d8cc-gdxvf telemetry icr.io/cpopen/turbonomic/kinesis-kafka-connect:8.12.5 turbonomic			

(T1105) Launch Ingress Remote File Copy Tools in Container

- La herramienta de copia de archivos remotos detectada dentro del contenedor sugiere un comportamiento anómalo que podría estar relacionado con la exfiltración de datos o con la posibilidad de recibir comandos desde un punto externo.
- El uso del comando curl para conectarse a un endpoint externo seguido de la ejecución de un script de verificación de estado podría ser un intento de ocultar actividades maliciosas dentro del contenedor.
- La severidad media indica que el evento tiene un impacto potencial, aunque no se confirma una actividad maliciosa directa. Sin embargo, es importante investigarlo para prevenir futuros ataques.

Mitigación

- Implementar políticas de red que restrinjan las conexiones salientes del contenedor a solo endpoints aprobados.
- Analizar la integridad del script healthcheck.sh y otros archivos críticos dentro del contenedor para detectar modificaciones no autorizadas.
- Implementar reglas adicionales de monitoreo y alertamiento para detectar actividades inusuales en el contenedor, especialmente relacionadas con el uso de herramientas de copia de archivos y comandos de red.

Workbench - Peripheral Device Enumeration in Container

The screenshot displays the Trend Vision One Workbench interface. The top navigation bar includes the product name, a case ID (WB-18641-20240815-00010), a timestamp (2024-09-02 11:47), and a user profile for 'BANCO MERCANTIL DEL NORTE S.A. INSTITUCIÓN DE BANCA MÚLTIPLE GRUPO FINANCIERO BA'. The left sidebar contains a 'Summary' section with details about the case, owners, and a 'Peripheral Device Enumeration in Container' event. The main area shows a timeline of events, with a highlighted event at 2024-08-14 21:54:04. The event details include a technique (T1120 - Peripheral Device Discovery), data source (Trend Vision One Container Security processor), and a list of commands executed, such as 'lsblk --list --noheadings...' and 'platform-python /opt/ansible/ansible/tmp/ansible-tmp-1723694043.798627-712184-51686832399039/AnsiballZ_setup.py'.

Trend Vision One™ | Workbench • WB-18641-20240815-00010 | 2024-09-02 11:47 | 99+ | BANCO MERCANTIL DEL NORTE S.A. INSTITUCIÓN DE BANCA MÚLTIPLE GRUPO FINANCIERO BA

Summary

Case: [Open new case](#)

Owners: None [Assign owner](#)

Peripheral Device Enumeration in Container

Executing specific commands to gather information about connected peripheral devices.

Score: 31

Impact scope: 1

Created: 2024-08-14 21:58:09

Automated responses: None [Execute playbook](#)

Highlights

Peripheral Device Enumeration in Container

Technique: T1120 - Peripheral Device Discovery

Data source / Trend Vision One Container Security processor:

2024-08-14 21:54:04 | [View event](#)

operator

(processCmd) lsblk --list --noheadings --path...

(k8sPodName) migration-operator-5bd87fd6...

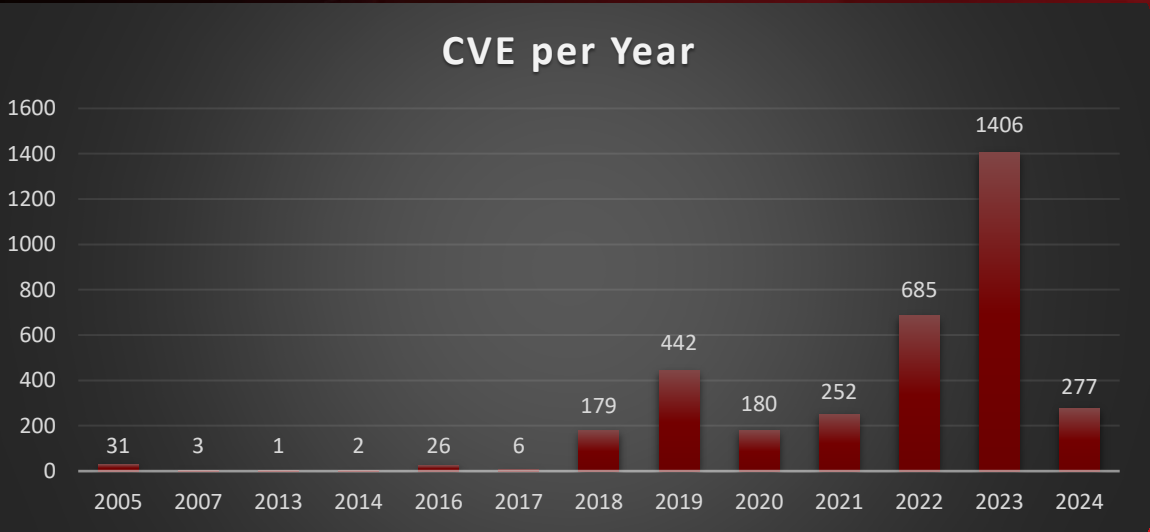
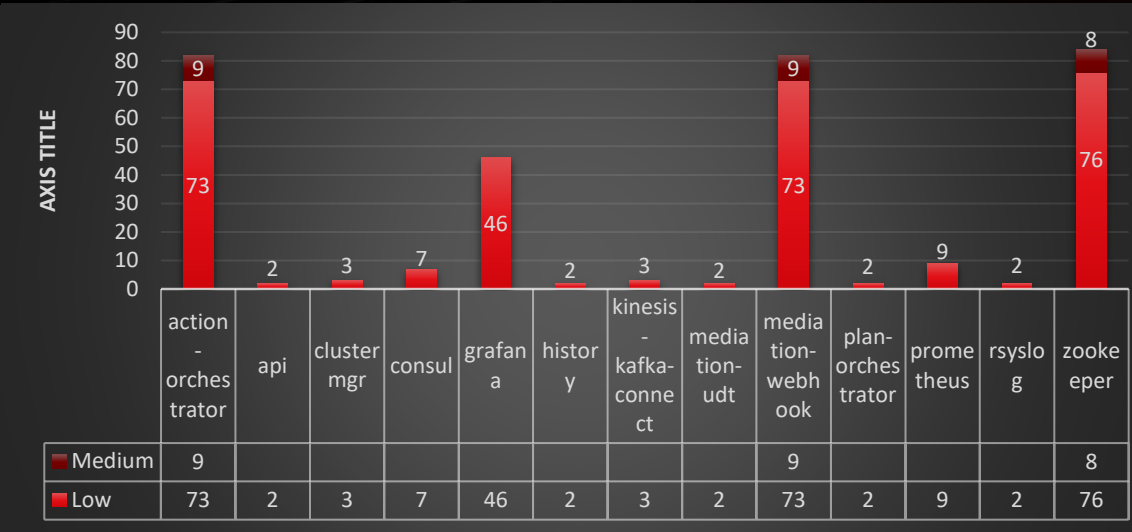
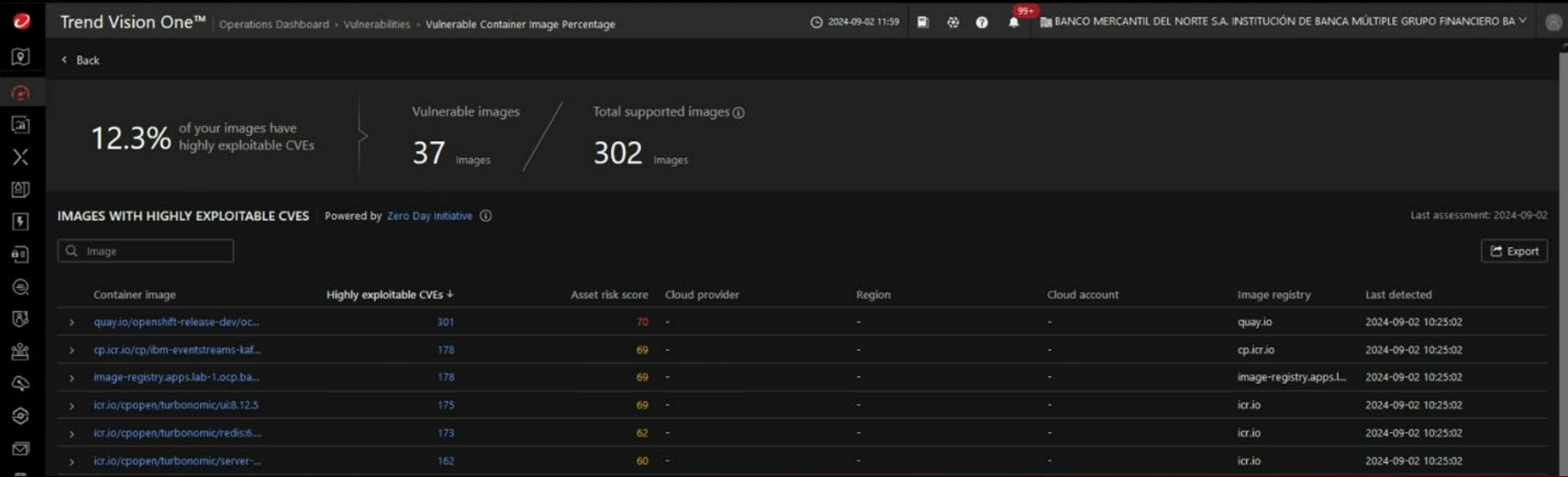
(clusterName) Cluster_prueba_120824

(parentCmd) platform-python /opt/ansible/a...

platform-python /opt/ansible/ansible/tmp/ansible-tmp-1723694043.798627-712184-51686832399039/AnsiballZ_setup.py

- Este evento indica que se han ejecutado comandos para enumerar dispositivos periféricos conectados en un contenedor. Este comportamiento puede ser legítimo en ciertos contextos de operación, pero también puede ser indicativo de actividades de reconocimiento maliciosas dentro del contenedor.
- La ejecución de comandos para descubrir dispositivos periféricos dentro de un contenedor puede ser un primer paso en un intento de reconocimiento más profundo o en la búsqueda de dispositivos vulnerables.

Container Vulnerability – Metrics



VULNERABILITIES - CVE-2022-47629



Asset Criticality	7
Package Name	libksba
Package Version	0:1.3.5-9.el8_6
Container Image ID	quay.io/openshift-release-dev/ocp-v4.0-art-dev
Container Image Digest	sha256:555aa8459c090a3b8120a22a7b46b6ce2e163294e4071836dc4778925aef2ec8

CVE-2022-47629

CVE Score v3 **9.8**

La vulnerabilidad **CVE-2022-47629** afecta a la biblioteca Libksba antes de la versión 1.6.3, y se trata de un **desbordamiento de entero** en el analizador de firmas CRL. Esto puede permitir a un atacante remoto ejecutar código arbitrario en el sistema o causar una denegación de servicio (DoS) al manipular de manera maliciosa un archivo de firma CRL (Certificate Revocation List)

IMPACTO

Un atacante podría ejecutar código malicioso en el sistema afectado, obteniendo así control total sobre el contenedor o la máquina virtual en la que se ejecute el contenedor vulnerable. Esto podría derivar en la instalación de backdoors, la ejecución de comandos arbitrarios y el uso del sistema comprometido para lanzar ataques adicionales dentro de la red interna.

Fix Available Openshift: <https://access.redhat.com/errata/RHSA-2024:4329>

VULNERABILITIES - CVE-2022-37832



Asset Criticality	7
Package Name	libksba
Package Version	0:1.3.5-9.el8_6
Image ID	quay.io/openshift-release-dev/ocp-v4.0-art-dev
Digest	sha256:555aa8459c090a3b8120a22a7b46b6ce2e163294e4071836dc4778925aef2ec8

CVE-2022-37832

CVE Score v3 **9.8**

La vulnerabilidad **CVE-2022-37832** se refiere a la presencia de una **contraseña root codificada** en el sistema Mutiny 7.2.0-10788, lo que representa un riesgo crítico de seguridad. Esta vulnerabilidad permite a los atacantes obtener acceso no autorizado al sistema utilizando esta contraseña predeterminada, lo que les da la capacidad de tomar el control total del sistema afectado

IMPACTO

Si esta vulnerabilidad es explotada, podría resultar en la pérdida completa del control del sistema, exfiltración de datos sensibles, y servir como puerta de entrada para ataques más amplios dentro de la red corporativa.

VULNERABILITIES - CVE-2024-6104



Asset Criticality	7
Package Name	libksba
Package Version	0:1.3.5-9.el8_6
Image ID	quay.io/openshift-release-dev/ocp-v4.0-art-dev
Digest	sha256:555aa8459c090a3b8120a22a7b46b6ce2e163294e4071836dc4778925aef2ec8

CVE-2024-6104

CVE Score

5.5

La vulnerabilidad **CVE-2024-6104** afecta a la biblioteca go-retryablehttp en versiones anteriores a la 0.7.7. Esta vulnerabilidad se debe a la falta de sanitización de las URLs al escribirlas en el archivo de registro (log file). Esto significa que credenciales de autenticación HTTP básica (HTTP basic auth credentials) podrían ser registradas inadvertidamente en los logs, lo que representa un riesgo de exposición de información sensible

IMPACTO

Esta vulnerabilidad puede ser particularmente crítica en entornos donde el acceso a los archivos de log no esté debidamente controlado. Es importante seguir las recomendaciones para evitar la exposición de credenciales y minimizar el impacto en la seguridad de la infraestructura.

Patched Package Version: 0.7.7



Trend Micro Vision One





Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Shift from Security Tools
to an **AI-Powered
Cybersecurity Platform**

Extended Detection and Response (XDR)



User and Identity



Email



Endpoints and Servers



Cloud Infrastructure



Applications



Code Repository



Data



Network



5G



ICS/OT

Email Security

Endpoint Security

Cloud Security

Network Security

Data Security

Identity Security

Risk Mitigation • IT Automation

Orchestration and Automation

Custom Playbooks • Case Management

Attack Surface Intelligence • Zero Day Initiative

Global Threat Intelligence

Threat Research • Big Data Analytics

AI Privacy and Ethics • AI Companion

AI Native Foundation

Generative AI • Custom LLM • Machine Learning

Managed Services

Ecosystem Integration

Blending Proactive & Reactive Security across the entire attack surface

Attack Surface Risk Management (ASRM)



Discovering
All Assets



Assessing
Cyber Risk



Prioritizing Risk
Mitigation Actions



Visualizing
Attack Pathways



AI/ML Driven
Remediation



Easing Compliance
and Operationalizing
Zero Trust



Extended Detection and Response (XDR)



Correlating Attacks
Cross-Layers



Coordinating Response
Cross-Vendors



Sweeping with
New Threat Intel



Powerful Hunting
and Forensic Tools



Augmenting Staff
with Companion AI



Automating Security
Response

Data Lake | Detection Logs and Activity Data

Endpoint



+ Protection

Identity



+ Protection

Email



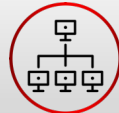
+ Protection

Cloud



+ Protection

Network



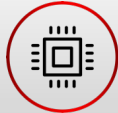
+ Protection

Data



+ Protection

OT



+ Protection

3rd Party



Third-Party Integrations

CATEGORIES

- Breach Attack Simulation (BAS)
- Cloud Services
- Firewall & Network Protection
- IT Service Management
- Identify & Access Management (IAM)
- SIEM
- SOAR
- Threat Intelligence (STIX/TAXII/MISP)
- Unified Endpoint Management
- Vulnerability Management

VENDORS



ASSOCIATED TREND VISION ONE APPS

- Attack Surface Discovery
- Attack Surface Risk Management
- Audit Log
- Case Management
- Container Security
- Email Asset Inventory
- Mobile Security
- Observed Attack Techniques
- Phishing Simulation Assessment
- Response Management
- Search
- Security Playbooks
- Service Gateway
- Threat Intelligence
- Workbench
- Zero Trust Secure Access

Flexible Pricing & Packaging



ASRM for Cloud

per cloud account

- Risk Assessment and Vulnerability Prioritization
- Cloud Asset Inventory and Cloud Graph
- Cloud Posture & API Visibility



ASRM for Devices

per Device

- Risk Assessment and Vulnerability Prioritization
- Asset Inventory and Asset Profile
- EASM, Account and User Activity



Protection

*Runtime protection and prevention
Detection and Response capabilities*

Licensed per

Endpoint Security

Runtime Detection & Protection for User Devices

Device

Server & Workload Security

Runtime Detection & Protection for hybrid workloads

workload

XDR Included

Container Security

Runtime Detection & Protection for hybrid containers

node
or
serverless container

Price: volume discounting available

Licensing: annual license; credit subscriptions; ELA (Enterprise License Agreement – **approval required prior to pitching**)





Thank you

