Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40

TLP: CLEAR

Incidente ID:	40
Fecha del reporte:	09/04/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en Docker Engine (AuthZ)
Herramienta de detección	N/A
Activo involucrado:	Docker Engine (Moby)
Tipo de incidente:	Alerta de Vulnerabilidad
Nivel de riesgo:	Alta

Objetivo:

Informar a las entidades del Ecosistema salud sobre la vulnerabilidad crítica CVE-2026-34040 en Docker Engine, este boletín es especialmente relevante para entornos que utilizan Docker Engine con plugins de autorización (AuthZ) habilitados, incluyendo plataformas cloud, entornos Kubernetes, pipelines CI/CD y cargas de trabajo de agentes de IA.

Descripción:

CVE-2026-34040 es una vulnerabilidad de alta severidad (CVSS 8.8) descubierta en Docker Engine que permite a un atacante eludir los mecanismos de autorización establecidos mediante plugins AuthZ. La vulnerabilidad fue descubierta e investigada por el equipo de Cyera Research Labs (investigador Vladimir Tokarev), así como de manera independiente por Asim Viladi Oglu Manizada, Cody y Oleh Konko.

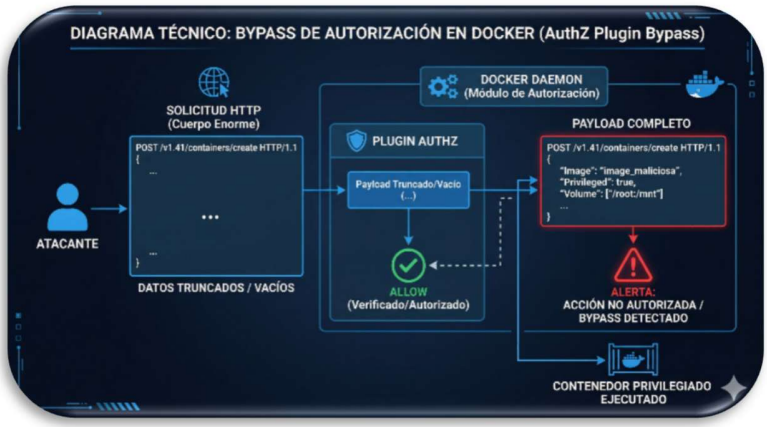
Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40

TLP: CLEAR

Identificador CVE	CVE-2026-34040
Severidad CVSS v3.1	8.8 (Alta)
Vector CVSS	AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Tipo de falla	CWE-288: Bypass de autenticación mediante canal alternativo
Descubierta por	Cyera Research Labs (Vladimir Tokarev) + investigadores independientes
Divulgación pública	Abril 2026
Parche disponible	Docker Engine v29.3.1 / Moby v29.3.1
Prerrequisito	Acceso al Docker API con AuthZ plugin habilitado

Esta vulnerabilidad es un fix incompleto de CVE-2024-41110, una falla de severidad máxima divulgada en julio de 2024. El parche original de CVE-2024-41110 abordaba el caso de solicitudes HTTP con cuerpo de longitud cero (0 bytes), pero no contemplo el caso contrario: solicitudes HTTP con cuerpos extremadamente grandes (superiores a 1 MB). Este descuido deja abierta una condición idéntica de bypass, pero aprovechando el límite superior en lugar del inferior.



La falla radica en un comportamiento inconsistente en el manejo del cuerpo (body) de solicitudes HTTP dentro de la arquitectura de Docker:

- Cuando el cuerpo de una solicitud HTTP al Docker API supera 1 MB, el middleware de Docker lo trunca silenciosamente antes de enviarlo al plugin de autorización AuthZ.
- Sin embargo, el Docker daemon sigue procesando la solicitud completa y sin modificar, ejecutando el payload original en su totalidad.
- El plugin AuthZ recibe un cuerpo vacío o truncado, interpreta que no hay acción riesgosa y permite la solicitud.
- El daemon ejecuta la solicitud completa, incluyendo instrucciones para crear un contenedor privilegiado con acceso al sistema de archivos del host.

Consecuencias de la Explotación

La explotación exitosa de CVE-2026-34040 puede resultar en impactos de máxima gravedad sobre la infraestructura comprometida:

Compromiso Total del Host

- Creación de contenedores privilegiados con montaje del filesystem raiz del host (/), otorgando acceso sin restricciones a todos los archivos del sistema.
- Escape del namespace de contenedor, obteniendo capacidades equivalentes a root sobre el sistema operativo anfitrión.
- Ejecución arbitraria de código y comandos directamente sobre el host.

Robo de Credenciales

- Extracción de credenciales de servicios cloud (AWS ~/.aws/credentials, GCP service accounts, Azure tokens).
- Robo de configuraciones de Kubernetes (~/.kube/config), permitiendo control sobre clusters K8s completos.

- Acceso a claves SSH privadas, tokens de API, secretos de aplicaciones y bases de datos.

Movimiento Lateral y Escalada

- Uso de credenciales robadas para pivotar a cuentas cloud, clusters Kubernetes y servidores de producción vía SSH.
- Compromiso de pipelines CI/CD que usan Docker como runtime de ejecución.
- En entornos con agentes de IA (e.g., OpenClaw u otros coding agents), el ataque puede ejecutarse de forma automatizada e invisible, sin intervención humana.

Impacto Organizacional

- Violación de datos sensibles de clientes, empleados y operaciones.
- Interrupción de servicios críticos por manipulación del host o los contenedores.
- Riesgo de cumplimiento normativo (GDPR, ISO 27001, SOC2, PCI-DSS).
- Dano reputacional y posibles implicaciones legales.

Modo de explotación y cadena de infección

El ataque se puede llevar a cabo mediante el siguiente flujo técnico detallado:

Fase 1: Reconocimiento y Acceso al Docker API

- El atacante obtiene acceso al Docker API, ya sea directamente al socket Unix /var/run/docker.sock, a través del TCP API (:2375 o :2376), o mediante un agente de IA con acceso programático al Docker API.
- Verifica la versión de Docker y si hay plugins AuthZ activos haciendo una petición a GET /version o GET /info.
- Comprueba que sus peticiones normales a /containers/create con --privileged son bloqueadas por el AuthZ plugin.

Fase 2: Construcción del Payload Malicioso

El atacante construye una solicitud HTTP POST al endpoint de creación de contenedores con las siguientes características criticas:

- El cuerpo JSON valido de la solicitud incluye la configuración maliciosa: contenedor privilegiado, montaje del filesystem del host y posiblemente --pid=host o --net=host.
- Se agrega relleno (padding) al cuerpo de la solicitud hasta que su tamaño total supere 1,048,576 bytes (1 MB). Este padding puede consistir en un campo JSON adicional con una cadena de caracteres arbitraria de gran longitud.
- La solicitud resultante es sintácticamente valida desde el punto de vista HTTP y Docker API, solo que excesivamente grande.

Ejemplo conceptual de la solicitud con padding:

```
POST /v1.41/containers/create HTTP/1.1 Content-Type: application/json Content-Length: 1100000 { "Image": "alpine", "HostConfig": { "Privileged": true, "Binds": ["/:/host"] }, "_padding": "AAAA...AAAA" (>1MB total) }
```

Fase 3: Bypass del Plugin de Autorización

- El middleware de Docker recibe la solicitud y, al detectar que el cuerpo supera 1 MB, lo trunca antes de pasarlo al plugin AuthZ.
- El plugin AuthZ recibe un cuerpo vacio o incompleto, no detecta la solicitud de contenedor privilegiado ni el montaje del host, y devuelve una respuesta de autorización positiva (allow).
- El Docker daemon, que mantiene la solicitud original intacta en memoria, procede a ejecutar el payload completo: crea el contenedor privilegiado con el montaje /:/host.

Fase 4: Ejecución de Comandos y Escalada

- El atacante ejecuta comandos dentro del contenedor privilegiado recién creado, accediendo al filesystem del host a través de /host.
- Lee y exfiltra archivos de credenciales: /host/root/.kube/config, /host/home/usuario/.aws/credentials, /host/etc/shadow, claves SSH, etc.

- Potencialmente modifica archivos del sistema del host (agregar usuario, instalar backdoor, modificar cron jobs) para establecer persistencia.

Fase 5: Pivoteo y Exfiltración

- Con las credenciales robadas, el atacante se conecta a clusters Kubernetes, cuentas cloud (AWS, GCP, Azure) y servidores de producción vía SSH.
- Puede escalar el ataque a toda la infraestructura orquestada, crear nuevos recursos cloud, modificar configuraciones o exfiltrar datos críticos.
- En el escenario con agentes de IA, todo este proceso puede ocurrir de forma automatizada sin intervención humana, iniciado por un repositorio malicioso analizado por el agente.

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40 **TLP: CLEAR**

Explicación de las Vulnerabilidades Relacionadas:

- **CVE-2026-34040 (Vulnerabilidad Principal)**

Descripción	Bypass del plugin de autorización AuthZ mediante solicitudes HTTP con cuerpo superior a 1 MB
Tipo (CWE)	CWE-288: Authentication Bypass Using an Alternate Path or Channel
Causa raíz	Inconsistencia en el manejo de cuerpos HTTP de gran tamaño: el middleware trunca el body antes del AuthZ plugin, pero el daemon ejecuta el payload completo
Impacto	Confidencialidad: Alto | Integridad: Alto | Disponibilidad: Alto
Productos afectados	Docker Engine (Moby) versiones < 29.3.1 con AuthZ plugins habilitados
Parche	Docker Engine / Moby version 29.3.1

- **CVE-2024-41110 (Vulnerabilidad Antecesora)**

Descripción	Bypass del plugin AuthZ con solicitudes HTTP de cuerpo de longitud cero (0 bytes)
Tipo (CWE)	CWE-288: Authentication Bypass Using an Alternate Path or Channel
Causa raíz	Cuando el cuerpo HTTP es 0 bytes, el daemon procesaba la solicitud sin enviársela al AuthZ plugin

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40 **TLP: CLEAR**

Severidad CVSS	10.0 (Critica)
Divulgación	Julio 2024
Relación con CVE-2026-34040	El parche de CVE-2024-41110 no contemplo el caso de cuerpos mayores a 1 MB, resultando en CVE-2026-34040

Mas allá de los CVEs específicos, existe una debilidad de diseño subyacente: los plugins AuthZ en Docker dependen de inspeccionar el cuerpo de las solicitudes HTTP para tomar decisiones de seguridad. Esta arquitectura introduce fragilidades inherentes cuando el sistema no garantiza que el cuerpo evaluado sea idéntico al ejecutado. Esto representa un patrón de falla que puede reaparecer en otras condiciones de borde no exploradas.

Relación con tácticas MITRE ATT&CK

La explotación de CVE-2026-34040 puede mapearse a las siguientes técnicas del framework MITRE ATT&CK for Containers (version 15):

Técnica ID	Nombre	Descripción en el contexto	Táctica
T1190	Exploit Public-Facing Application	El atacante explota el endpoint HTTP del Docker API expuesto a la red.	Reconocimiento / Acceso Inicial
T1610	Deploy Container	Creación de contenedores privilegiados con montaje del filesystem del host mediante la solicitud manipulada.	Ejecución

CSIRT Salud

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40

TLP: CLEAR

Técnica ID	Nombre	Descripción en el contexto	Táctica
T1548.001	Abuse Elevation Control Mechanism: Setuid/Setgid	Escape del namespace de contenedor al obtener privilegios root sobre el host.	Escalada de Privilegios
T1005	Data from Local System	Acceso y exfiltración de credenciales, kubeconfig y secretos del host montado.	Recopilación
T1552.001	Credentials In Files	Lectura de archivos de credenciales (AWS, kubectl, SSH) desde el filesystem del host.	Acceso a Credenciales
T1036	Masquerading	El payload malicioso se oculta en solicitudes HTTP legítimas con relleno de bytes.	Evasión de Defensa
T1059	Command and Scripting Interpreter	Ejecución de comandos arbitrarios dentro del contenedor privilegiado.	Ejecución
T1078	Valid Accounts	Uso de credenciales robadas del host para pivotear a otros sistemas (K8s, cloud, SSH).	Persistencia / Movimiento Lateral

La cadena de ataque completa sigue el patrón: Reconocimiento -> Acceso Inicial -> Ejecución -> Escalada de Privilegios -> Evasión -> Acceso a Credenciales -> Movimiento Lateral -> Recopilación -> Exfiltración.

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40 **TLP: CLEAR**

Activos o versiones afectados:

La vulnerabilidad afecta de forma específica y exclusiva a la siguiente versión del producto:

- Docker Engine / framework Moby: Versiones anteriores a la 29.3.1.
- Afecta a implementaciones empresariales independientemente del plugin de autorización utilizado, impactando potencialmente distribuciones empaquetadas como Ubuntu, Amazon Linux, entre otras, que corran versiones de Docker vulnerables.

Producto	Versión	Estado
Docker Engine / Moby	1.10 hasta 29.3.0 (con AuthZ plugins habilitados)	Vulnerable
Docker Engine / Moby	29.3.1 o posterior	Parcheado
Docker Desktop (Windows/macOS/Linux)	Versiones con Engine < 29.3.1	Vulnerable
Docker Desktop (Windows/macOS/Linux)	Actualizar a versión con Engine 29.3.1+	Parcheado
Mirantis Container Runtime (MCR)	Versiones < 25.0.8 con AuthZ	Potencialmente afectado

IMPORTANTE: Un entorno Docker es vulnerable a CVE-2026-34040 **UNICAMENTE** si cumple ambas condiciones simultáneamente:

- Ejecuta Docker Engine en una versión anterior a 29.3.1 (incluidas versiones tan antiguas como 1.10).
- Tiene uno o más plugins de autorizacion AuthZ configurados y activos (OPA, Prisma Cloud, plugins personalizados, etc.).

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40 **TLP: CLEAR**

Los entornos Docker que no utilizan plugins AuthZ NO están afectados por esta vulnerabilidad. Sin embargo, se recomienda actualizar de todas formas como buena práctica de seguridad.

Indicadores de compromiso:

A continuación se presentan los indicadores de compromiso generales y detectados asociados a la explotación de CVE-2026-34040:

Tipo	Categoría	Indicador
Red	Tráfico HTTP	Solicitudes POST al Docker API (/v1.*/containers/create) con body > 1 MB seguidas de respuesta 201
Red	Tráfico HTTP	Content-Length anormalmente elevado (>1 048 576 bytes) en endpoint Docker API
Host	Proceso	Ejecución de docker run con flags --privileged --pid=host o -v /:/host
Host	Filesystem	Montajes en /proc/1/root/ o /host desde dentro de contenedor
Host	Logs Docker	Ausencia de registro de AuthZ en docker daemon logs tras creación de contenedor privilegiado
Host	Archivo	Lectura de ~/.kube/config, ~/.aws/credentials, /etc/shadow desde proceso de contenedor
Cloud	API Calls	Llamadas inesperadas a AWS/GCP/Azure desde IPs o roles asociados al host Docker comprometido
K8s	kubectl	Creación de pods privilegiados o uso de kubeconfig desde host Docker no autorizado

Patrones de Comportamiento Sospechoso Adicionales

- Proceso dockerd generando contenedores sin registro previo en logs de AuthZ plugin.
- Nuevos procesos hijo de dockerd con --privileged en entornos que lo tienen prohibido por politica.
- Acceso a /proc/[pid]/root o /sys desde dentro de un contenedor.
- Incremento anomalo en el tráfico saliente del host Docker hacia IPs externas no habituales.
- Creación de tareas cron, modificación de /etc/passwd o /etc/sudoers desde proceso de contenedor.
- Ejecución de herramientas de reconocimiento (nmap, curl, wget) desde dentro de contenedores no esperados.

Recomendaciones de mitigación:

Para identificar posibles explotaciones de CVE-2026-34040 en su entorno se recomienda implementar las siguientes medidas:

Monitoreo de Red:

- Implementar reglas en IDS/IPS y WAF para detectar solicitudes HTTP POST al Docker API con Content-Length superior a 1,048,576 bytes.
- Verificar solicitudes a /containers/create con cuerpos anómalamente grandes seguidas de respuesta HTTP 201.
- Monitorear tráfico de red saliente inusual desde el host Docker hacia infraestructura cloud o IPs externas desconocidas.

Monitoreo de Host y Contenedores:

- Habilitar auditd para registrar accesos a /var/run/docker.sock y detectar procesos no autorizados que interactúen con el socket Docker.
- Configurar alertas para la creación de contenedores con flags --privileged, --pid=host, -v /:/host.
- Monitorear accesos a archivos sensibles del host (/etc/shadow, ~/.kube/config, ~/.aws/credentials) desde procesos de contenedor.
- Revisar periodicamente la lista de contenedores en ejecucion (docker ps) para identificar contenedores no autorizados o no documentados.

Monitoreo de Logs:

- Verificar que los logs del AuthZ plugin registren TODAS las solicitudes a endpoints críticos del Docker API.
- Alertar si hay solicitudes exitosas al Docker API sin el correspondiente registro de autorización en el plugin AuthZ.
- Integrar logs de Docker daemon con SIEM (Splunk, Elastic, etc.) para correlación de eventos.

Recomendación	Prioridad
Parchear Docker Engine a v29.3.1+	INMEDIATA
Restringir acceso al Docker socket/API (TLS, firewall, usuario no root)	INMEDIATA
Activar modo rootless de Docker o --userns-remap	ALTA
Implementar monitoreo de tráfico HTTP al Docker API (cuerpos >1 MB)	ALTA
Revisar y auditar contenedores privilegiados en ejecución	ALTA
Habilitar auditd para monitorear acceso a /var/run/docker.sock	MEDIA

Alerta Vulnerabilidad
Vulnerabilidad en Docker Engine (AuthZ)

CSIRTSALUD-AV-20260409-40 **TLP: CLEAR**

Recomendación	Prioridad
Revisar logs de AuthZ plugins para detectar solicitudes anómalas	MEDIA
Rotar credenciales cloud y kubeconfig como medida preventiva	MEDIA
Implementar políticas de red para limitar comunicación saliente del host	MEDIA
Capacitar equipos DevOps sobre buenas prácticas de seguridad en Docker	BAJA

Si se sospecha o confirma una explotación de CVE-2026-34040:

- Aislar inmediatamente el host Docker comprometido de la red de producción.
- Detener todos los contenedores en ejecución y documentar su configuración para análisis forense.
- Rotar TODAS las credenciales potencialmente expuestas: cloud (AWS/GCP/Azure), Kubernetes, SSH, bases de datos, tokens de API.
- Revisar logs de actividad de los últimos 30 días en los servicios cloud y Kubernetes para identificar accesos no autorizados.
- Reinstalar el host desde cero (o restaurar desde snapshot limpio) en lugar de intentar limpiar el sistema comprometido.
- Actualizar a Docker Engine 29.3.1 antes de reintegrar el host al entorno de producción.

Fuentes:

- CISA — Known Exploited NVD — National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2026-21643
- Fortinet PSIRT Advisory: https://www.fortiguard.com/psirt

- NVD - National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2026-34040
- GitHub Advisory (Moby): https://github.com/moby/moby/security/advisories/GHSA-x744-4wpc-v9h2
- Cyera Research Labs - Reporte original del investigador Vladimir Tokarev
- The Hacker News: Docker CVE-2026-34040 Lets Attackers Bypass Authorization and Gain Host Access
- eSecurity Planet: Docker Flaw Lets Attackers Bypass Security Controls and Take Over Hosts
- CVE Antecesora: CVE-2024-41110 (Julio 2024) - https://nvd.nist.gov/vuln/detail/CVE-2024-41110
- MITRE ATT&CK for Containers: https://attack.mitre.org/matrices/enterprise/containers/
- Docker Security Documentation: https://docs.docker.com/engine/security/
- Docker Rootless Mode: https://docs.docker.com/engine/security/rootless/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.