Resumen de Cambios Realizados con el apoyo de Docker Bench Security

Las siguientes acciones realizadas han modificado intencionalmente la propiedad y los permisos de ciertos archivos y directorios críticos de Docker para generar advertencias en lugar de correcciones en Docker Bench Security.

**3.1 - Ensure that the docker.service file ownership is set to root**

****

Estado Actual: [**WARN**] Motivo: Propiedad incorrecta para /lib/systemd/system/docker.service.

Acciones Realizadas:

-Cambiamos la propiedad del archivo docker.service a nobody:nogroup.

*sudo chown nobody:nogroup /lib/systemd/system/docker.service*

**3.2 - Ensure that docker.service file permissions are appropriately set**

****

Estado Actual: [**WARN**] Motivo: Permisos incorrectos para /lib/systemd/system/docker.service.

Acciones Realizadas:

Cambiamos los permisos del archivo docker.service a 777.

*sudo chmod 777 /lib/systemd/system/docker.service*

**3.5 - Ensure that the /etc/docker directory ownership is set to root**

****

Estado Actual: [**WARN**] Motivo: Propiedad incorrecta para /etc/docker.

Acciones Realizadas:

Cambiamos la propiedad del directorio /etc/docker a nobody:nogroup.

*sudo chown nobody:nogroup /etc/docker*

**3.6 - Ensure that /etc/docker directory permissions are set to 755 or more restrictively**

****

Estado Actual: [**WARN**] Motivo: Permisos incorrectos para /etc/docker.

Acciones Realizadas:

Cambiamos los permisos del directorio /etc/docker a 777.

*sudo chmod 777 /etc/docker*

**3.15 - Ensure that the Docker socket file ownership is set to root**

****

Estado Actual: [**WARN**] Motivo: Propiedad incorrecta para /var/run/docker.sock.

Acciones Realizadas:

Cambiamos la propiedad del archivo docker.sock a nobody:nogroup.

*sudo chown nobody:nogroup /var/run/docker.sock*

**3.16 - Ensure that the Docker socket file permissions are set to 660 or more restrictively**

****

Estado Actual: [**WARN**] Motivo: Permisos incorrectos para /var/run/docker.sock.

Acciones Realizadas:

Cambiamos los permisos del archivo docker.sock a 777.

sudo chmod 777 /var/run/docker.sock

Resumen de Cambios Realizados con el apoyo de Trivy

**Vulnerabilidad: CVE-2022-46175**

**Biblioteca Afectada:** json5

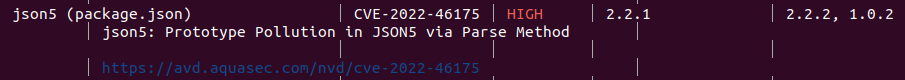
**Versión Afectada:** 2.2.1

**Versión Fijada:** 2.2.3, 1.0.2

**Severidad:** Alta (**HIGH**)

Descripción: La vulnerabilidad CVE-2022-46175 en la biblioteca json5 es una vulnerabilidad de contaminación de prototipo **(*Prototype Pollution***). Esto ocurre cuando un atacante puede modificar el prototipo de objetos JavaScript, lo que puede afectar toda la aplicación y potencialmente permitir la ejecución de código arbitrario.

**Detalles Técnicos:**

****

**Prototipo de Contaminación:** Esta vulnerabilidad permite a un atacante modificar el prototipo de objetos a través de datos de entrada manipulados.

**Ejemplo:** Un atacante podría enviar un payload malicioso que modifique el prototipo de todos los objetos, añadiendo propiedades o métodos inesperados que pueden ser explotados.

**Impacto:**

**Ejemplo de Exploit:**

*const JSON5 = require('json5');*

*const payload = '{"\_\_proto\_\_": {"admin": true}}';*

*const obj = JSON5.parse(payload);*

console.log(obj.admin); // true

console.log({}.admin); // true, contaminación del prototipo

En este ejemplo, la propiedad admin se agrega al prototipo de todos los objetos, lo que puede tener efectos perjudiciales en toda la aplicación.

**Instalar json5 Versión Vulnerable:**

Instala json5 en su versión vulnerable:

*npm install json5@2.2.1*

Modificar en el archivo “**package-lock.json**” dentro de “getting-started” a la versión vulnerable de json5:



Al modificar el archivo forzando la versión “2.2.1” Trivy detectará el fallo.