Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 010	Fecha: 11-01-2023
		Página 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Fallo critico de seguridad encontrada en la biblioteca "jsonwebtoken" utilizada por más de 22 000 proyectos		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet, Correo electrónico, Redes Sociales		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

Descripción

Se ha revelado una falla de seguridad de alta gravedad en la biblioteca jsonwebtoken (JWT) de código abierto que, si se explota con éxito, podría conducir a la ejecución remota de código en un servidor de destino.

Al explotar esta vulnerabilidad, los atacantes podrían lograr la ejecución remota de código (RCE) en un servidor que verifica una solicitud de token web JSON (JWT) creada con fines maliciosos.

DETALLES:

Registrado como CVE-2022-23529 (puntaje CVSS: 7.6), el problema afecta a todas las versiones de la biblioteca, incluida la 8.5.1 y anteriores, y se solucionó en la versión 9.0.0 enviada el 21 de diciembre de 2022.

jsonwebtoken, desarrollado y mantenido por Auth0 de Okta, es un módulo de JavaScript que permite a los usuarios decodificar, verificar y generar tokens web JSON como un medio de transmisión segura de información entre dos partes para autorización y autenticación.

Por lo que, la capacidad de ejecutar código malicioso en un servidor podría romper las garantías de confidencialidad e integridad, lo que podría permitir que un mal actor sobrescriba archivos arbitrarios en el host y realice cualquier acción de su elección utilizando una clave secreta envenenada.

A medida que el software de código abierto emerge cada vez más como una vía de acceso inicial lucrativa para que los actores de amenazas realicen ataques a la cadena de suministro, es crucial que los usuarios intermedios identifiquen, mitiguen y corrijan de manera proactiva las vulnerabilidades en dichas herramientas.

RECOMENDACIONES:

- Para detectar las vulnerabilidades de código abierto Google lanzo una herramienta llamada OSV-Scanner que ayuda a identificar todas las dependencias transitivas de un proyecto y resaltar las deficiencias relevantes que lo afectan.

Fuentes de información	▪ hxxps://thehackernews.com/2023/01/critical-security-flaw-found-in.html ▪ hxxps://thehackernews.com/2022/12/google-launches-largest-distributed.html