	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°266	Fecha: 07-11-2023
		Página: 8 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el software OpenSSL		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **MEDIA** de tipo error de gestión de recursos en el software OpenSSL. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-5678 de tipo error de gestión de recursos, existe debido a una gestión inadecuada de los recursos internos dentro de las funciones DH_generate_key() y DH_check_pub_key(). Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y realizar un ataque de DoS.

A. Productos afectados:

- OpenSSL: 1.0.2 - 3.1.4

3. RECOMENDACIÓN:

- Actualizar el paquete afectado con la última versión de software disponible que el proveedor lance para abordar esta vulnerabilidad.

Fuente de Información:	• hxxp://www.openssl.org/news/secadv/20231106.txt