Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 032	Fecha: 06-02-2023
		Página 4 de 17

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades en OpenSSH Server		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

OpenSSH lanza una nueva versión e informa de dos (02) vulnerabilidades corregidas con la misma.

ANTECEDENTES:

- OpenSSH, es la principal herramienta de conectividad para el inicio de sesión remoto con el protocolo SSH. Cifra todo su tráfico evitando la interceptación ilegal, el secuestro de conexiones y otros ataques por parte de terceros.

DETALLES:

- El 02 de Febrero de 2023, OpenSSH anunció su nueva versión 9.2, la cual corrige dos vulnerabilidades en sus versiones anteriores.

- La vulnerabilidad double-free que es introducido en la versión de Openssh 9.1, puede ser activado por un atacante no autenticado en la configuración predeterminada; sin embargo, no se cree que esto sea explotable, y ocurre en el proceso de autorización previa sin privilegios.

- La otra vulnerabilidad permite a un atacante remoto eludir las restricciones de seguridad implementadas debido a un error lógico al analizar la opción “PermitRemoteOpen”, la cual ignoraría su primer argumento a menos que fuera una de las palabras especiales: "cualquiera" o "ninguno", lo que hace que la lista de permisos no se abra si no se especifica un permiso. Las versiones vulnerables de OpenSSH son: 8.7 a 9.1

RECOMENDACIONES:

- Actualizar OpenSSH a su versión 9.2.
- Evitar descargar aplicaciones de sitios no confiables.
- Las estaciones de trabajo deben contar con las ultimas actualizaciones de software (Sistema operativo y antivirus).

Fuentes de información	▪ hxxps:// https://www.openssh.com/releasenotes.html#9.2 ▪ Análisis propio de fuentes abiertas.