	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°034	Fecha: 08-02-2024
		Página: 11 de 20

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en la herramienta Tenable Nessus		
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 dos vulnerabilidades de severidad **MEDIA** de tipo secuencia de comandos entre sitios e inyección SQL en la herramienta Tenable Nessus. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto robar información confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y ejecutar comandos arbitrarios.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-0955 de tipo secuencia de comandos entre sitios, existe debido a una limpieza insuficiente de los datos proporcionados por los usuarios. Un usuario remoto puede inyectar y ejecutar código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-09571 de tipo inyección SQL, existe debido a una limpieza insuficiente de los datos proporcionados por los usuarios. Un usuario remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

A. Productos afectados:

- Tenable Nessus: 10.6.0 - 10.6.3.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.tenable.com/security/tns-2024-01