DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 029**	**Fecha: 02-02-2023**
		Página 6 de 34

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de escalada de privilegios en productos Tenable		
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

1. **Resumen:**

- Tenable, Inc. ha reportado una vulnerabilidad de severidad CRÍTICA de tipo escalada de privilegios que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir que un actor malicioso con suficientes permisos modifique las variables del entorno y abuse de un complemento afectado para aumentar los privilegios.

2. **Detalles:**

- La vulnerabilidad de severidad critica registrada como CVE-2023-0524 de escalada de privilegios, podría permitir que un actor malicioso con suficientes permisos modifique las variables del entorno y abuse de un complemento afectado para aumentar los privilegios.

3. **Productos afectados:**

- Tenable.io sin el ultimo parche de seguridad.
- Tenable.sc sin el último parche de seguridad.
- Nessus sin el último parche de seguridad.

4. **Solución:**

- Tenable recomienda actualizar los productos afectados con la última versión de software disponible que corrige esta vulnerabilidad.
- Asimismo, se recomienda consultar el boletín de seguridad para obtener parches (Boletín de seguridad de Tenable TNS-2023-04 del 30 de enero de 2023).

Fuentes de información	▪ hxxps://www.tenable.com/security/tns-2023-04 ▪ hxxps://www.cve.org/CVERecord?id=CVE-2023-0524