DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°007**	**Fecha: 08-01-2024**
		Página: 6 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades de escalada de privilegios de Cisco Identity Services Engine		
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:

Cisco ha reportado dos vulnerabilidades de severidad **MEDIA** de tipo escalada de privilegios que afectan a múltiples en Cisco Identity Services Engine (ISE). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante autenticado realizar ataques de escalada de privilegios para leer o modificar archivos arbitrarios en el sistema operativo subyacente. Para explotar estas vulnerabilidades, un atacante debe tener privilegios válidos de nivel de administrador en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20193 de tipo escalada de privilegios en el enrutador de servicios integrado (ESR) de Cisco ISE podría permitir que un atacante local autenticado lea, escriba o elimine archivos arbitrarios en el sistema operativo subyacente y escale sus privilegios a root. Para aprovechar esta vulnerabilidad, un atacante debe tener privilegios válidos de nivel de administrador en el dispositivo afectado. Esta vulnerabilidad se debe a una gestión inadecuada de privilegios en la consola ESR. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud diseñada a un dispositivo afectado. Un exploit exitoso podría permitir al atacante elevar sus privilegios a root y leer, escribir o eliminar archivos arbitrarios del sistema operativo subyacente del dispositivo afectado.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20194 de tipo escalada de privilegios en la API ERS de Cisco ISE podría permitir que un atacante remoto autenticado lea archivos arbitrarios en el sistema operativo subyacente de un dispositivo afectado. Para aprovechar esta vulnerabilidad, un atacante debe tener privilegios válidos de nivel de administrador en el dispositivo afectado. Esta vulnerabilidad se debe a una gestión inadecuada de privilegios en la API de ERS. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud diseñada a un dispositivo afectado. Un exploit exitoso podría permitir al atacante elevar sus privilegios más allá de la esfera de su nivel de acceso previsto, lo que le permitiría obtener información confidencial del sistema operativo subyacente.

Las vulnerabilidades no dependen unas de otras; La explotación de una de las vulnerabilidades no es necesaria para explotar la otra vulnerabilidad. Además, una versión de software que se ve afectada por una de las vulnerabilidades puede no verse afectada por la otra vulnerabilidad.

A. Productos afectados:

- La vulnerabilidad CVE-2023-20193 afecta a los dispositivos Cisco si ejecutan una versión vulnerable de Cisco ISE (2.7 y anteriores, 3.0, 3.1, y 3.2) y tienen habilitado el enrutador de servicio integrado (ESR).
- La vulnerabilidad CVE-2023-20194 afecta a los dispositivos Cisco si ejecutan una versión vulnerable de Cisco ISE (2.7 y anteriores, 3.0, 3.1, y 3.2) y tienen habilitado los servicios RESTful externos (ERS).

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que brinde el proveedor cisco para abordar esta vulnerabilidad. No existen soluciones alternativas que aborden estas vulnerabilidades.
- Restringir el acceso a la consola y el acceso web del administrador, ya que estas vulnerabilidades solo pueden ser aprovechadas por usuarios válidos y autorizados de Cisco ISE.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-KJLp2Aw