Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°212**	**Fecha: 08-09-2023**
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Cisco advierte sobre VPN de día cero explotada por bandas de ransomware		
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 advierte sobre una vulnerabilidad de día cero CVE-2023-20269 en su Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD) que es explotada activamente por operaciones de ransomware para obtener acceso inicial a las redes corporativas.

El mes pasado, BleepingComputer informó que la banda de ransomware Akira estaba violando las redes corporativas casi exclusivamente a través de dispositivos VPN de Cisco, y la firma de ciberseguridad SentinelOne especuló que podría deberse a una vulnerabilidad desconocida.

Una semana después, Rapid7 informó que la operación de ransomware Lockbit también aprovechó un problema de seguridad no documentado en los dispositivos VPN de Cisco además de Akira. Sin embargo, la naturaleza exacta del problema seguía sin estar clara.

En ese momento, Cisco publicó una advertencia de que las infracciones se llevaron a cabo mediante fuerza bruta en credenciales en dispositivos sin MFA configurado.

Esta semana, Cisco confirmó la existencia de una vulnerabilidad de día cero utilizada por estas bandas de ransomware y proporcionó soluciones en un boletín de seguridad provisional.

Sin embargo, las actualizaciones de seguridad para los productos afectados aún no están disponibles.

2. DETALLES:

La vulnerabilidad de día cero de gravedad media afecta la función VPN de Cisco ASA y Cisco FTD, lo que permite a atacantes remotos no autorizados realizar ataques de fuerza bruta contra cuentas existentes.

Al acceder a esas cuentas, los atacantes pueden establecer una sesión VPN SSL sin cliente en la red de la organización violada, lo que puede tener distintas repercusiones según la configuración de red de la víctima.

La falla CVE-2023-20269 se encuentra dentro de la interfaz de servicios web de los dispositivos Cisco ASA y Cisco FTD, específicamente las funciones que se ocupan de las funciones de autenticación, autorización y contabilidad (AAA).

La falla se debe a la separación inadecuada de las funciones AAA y otras características del software. Esto conduce a escenarios en los que un atacante puede enviar solicitudes de autenticación a la interfaz de servicios web para afectar o comprometer los componentes de autorización.

Dado que estas solicitudes no tienen limitación, el atacante puede utilizar credenciales de fuerza bruta utilizando innumerables combinaciones de nombre de usuario y contraseña sin tener una tasa limitada ni bloquearse por abuso.

Para que los ataques de fuerza bruta funcionen, el dispositivo Cisco debe cumplir las siguientes condiciones:

Al menos un usuario está configurado con una contraseña en la base de datos LOCAL o puntos de autenticación de administración HTTPS a un servidor AAA válido.

SSL VPN está habilitado en al menos una interfaz o IKEv2 VPN está habilitado en al menos una interfaz.

Si el dispositivo objetivo ejecuta la versión 9.16 del software Cisco ASA o anterior, el atacante puede establecer una sesión VPN SSL sin cliente sin autorización adicional tras una autenticación exitosa.

Para establecer esta sesión VPN SSL sin cliente, el dispositivo de destino debe cumplir estas condiciones:

El atacante tiene credenciales válidas para un usuario presente en la base de datos LOCAL o en el servidor AAA utilizado para la autenticación de administración HTTPS. Estas credenciales podrían obtenerse mediante técnicas de ataque de fuerza bruta.

El dispositivo ejecuta el software Cisco ASA versión 9.16 o anterior.

SSL VPN está habilitado en al menos una interfaz.

El protocolo VPN SSL sin cliente está permitido en DfltGrpPolicy.

3. RECOMENDACIONES:

- Actualizar el paquete afectado con la última versión de software disponible que Cisco lanzará para abordar esta vulnerabilidad
- Utilizar DAP (Políticas de acceso dinámico) para detener los túneles VPN con DefaultADMINGroup o DefaultL2LGroup.
- Denegar el acceso con la política de grupo predeterminada ajustando vpn-simultaneous-logins para DfltGrpPolicy a cero y asegurarse que todos los perfiles de sesión de VPN apunten a una política personalizada.
- Implementar restricciones de bases de datos de usuarios LOCALES bloqueando usuarios específicos en un único perfil con la opción 'bloqueo de grupo' y evitar configuraciones de VPN estableciendo 'vpn-simultaneous-logins' en cero.
- Proteger los perfiles VPN de acceso remoto predeterminados apuntando todos los perfiles no predeterminados a un servidor AAA sumidero (servidor LDAP ficticio) y habilitar el registro para detectar posibles incidentes de ataque con anticipación.
- Habilitar la autenticación multifactor para establecer conexiones VPN.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/cisco-warns-of-vpn-zero-day-exploited-by-ransomware-gangs/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°212	Fecha: 08-09-2023
		Página: 6 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades de escalada de privilegios de Cisco ISE		
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 afecta a Cisco Identity Services Engine (ISE). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante autenticado 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. Para aprovechar 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 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. El ESR no está habilitado de forma predeterminada y debe tener licencia.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20194 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. El ERS no está habilitado de forma predeterminada.

Cabe indicar que estas 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.

Estas vulnerabilidades solo pueden ser aprovechadas por usuarios válidos y autorizados de Cisco ISE.

A. Productos afectados:

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

3. RECOMENDACIÓN:

- Actualizar el software afectado con la última versión de software disponible que Cisco ha lanzado para abordar estas vulnerabilidades.

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