	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°234	Fecha: 04-10-2023
		Página: 5 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos Cisco		
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 múltiples vulnerabilidades de severidad **CRÍTICA** y **ALTA** de tipo credenciales estáticas, elevación de privilegios y validación incompleta que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante no autenticado / autenticado ejecutar comandos arbitrarios como usuario root y generar una condición de denegación de servicio (DoS) debido a una alta utilización de la CPU. Para aprovechar estas vulnerabilidades, un atacante debe tener una cuenta válida en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-20101 en Cisco Emergency Responder, podría permitir que un atacante remoto no autenticado inicie sesión en un dispositivo afectado utilizando la cuenta raíz, que tiene credenciales estáticas predeterminadas que no se pueden cambiar ni eliminar. Esta vulnerabilidad se debe a la presencia de credenciales de usuario estáticas para la cuenta raíz que normalmente están reservadas para su uso durante el desarrollo. Un exploit exitoso podría permitir al atacante iniciar sesión en el sistema afectado y ejecutar comandos arbitrarios como usuario root.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2021-1572 en ConfD, podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el nivel de la cuenta bajo la cual se ejecuta ConfD, que usualmente es root. Para aprovechar esta vulnerabilidad, un atacante debe tener una cuenta válida en el dispositivo afectado. La vulnerabilidad existe porque el software afectado ejecuta incorrectamente el servicio de usuario SFTP en el nivel de privilegio de la cuenta que se estaba ejecutando cuando se habilitó el servidor Secure Shell (SSH) integrado de ConfD para CLI. Si el servidor SSH integrado de ConfD no estaba habilitado, el dispositivo no se ve afectado por esta vulnerabilidad. Un exploit exitoso podría permitir al atacante elevar los privilegios al nivel de la cuenta bajo la cual se ejecuta ConfD, que comúnmente es root. De forma predeterminada, todos los usuarios de ConfD tienen este acceso si el servidor está habilitado.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2021-1572 en Cisco Network Services Orchestrator (NSO), podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el nivel de la cuenta bajo la cual se ejecuta Cisco NSO, que es raíz de forma predeterminada. Para aprovechar esta vulnerabilidad, un atacante debe tener una cuenta válida en un dispositivo afectado. La vulnerabilidad existe porque el software afectado ejecuta incorrectamente el servicio de usuario SFTP en el nivel de privilegio de la cuenta que se estaba ejecutando cuando se habilitó el servidor SSH integrado de NSO para CLI. Si el servidor SSH integrado de NSO no estaba habilitado, el dispositivo no se ve afectado por esta vulnerabilidad. Un atacante con privilegios de bajo nivel podría aprovechar esta vulnerabilidad autenticándose en un dispositivo afectado y emitiendo una serie de comandos en la interfaz SFTP.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-20259 en un punto final API de múltiples productos de Comunicaciones Unificadas de Cisco, podría permitir que un atacante remoto no autenticado genere una condición de DoS debido a una alta utilización de la CPU, lo que podría afectar el acceso a la interfaz de administración basada en web y causar retrasos en el procesamiento de llamadas. Esta API no se utiliza para la administración de dispositivos y es poco probable que se utilice en las operaciones normales del dispositivo. Esta vulnerabilidad se debe a una autenticación de API incorrecta y a una validación incompleta de la solicitud de API. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada a una API específica en el dispositivo.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20235 en la función de flujo de trabajo de desarrollo de aplicaciones en el dispositivo para la infraestructura de alojamiento de aplicaciones Cisco IOx en el software Cisco IOS XE, podría permitir que un atacante remoto autenticado acceda al sistema operativo subyacente como usuario raíz. Esta vulnerabilidad existe porque los contenedores Docker con la opción de tiempo de ejecución privilegiado no se bloquean cuando están en modo de desarrollo de aplicaciones. Un atacante podría aprovechar esta vulnerabilidad utilizando la CLI de Docker para acceder a un dispositivo afectado. El flujo de trabajo de desarrollo de aplicaciones está destinado a usarse únicamente en sistemas de desarrollo y no en sistemas de producción.

A. Productos afectados:

- La vulnerabilidad CVE-2023-20101 afecta a Cisco Emergency Responder versión 12.5(1)SU4.
- La vulnerabilidad CVE-2021-1572 afecta a las versiones 7.4 a 8.1.3 de ConfD si el servidor SSH integrado para CLI está habilitado.
- La vulnerabilidad CVE-2021-1572 afecta a las versiones 5.4 a 6.1.3 de Cisco NSO si el servidor SSH integrado de NSO para CLI está habilitado.
- La vulnerabilidad CVE-2023-20259 afecta a los siguientes productos de Cisco independientemente de la configuración del dispositivo:
  - Cisco Emergency Responder Release, versión 14SU3.
  - Cisco Prime Collaboration Deployment Release, versión 14SU3.
  - Cisco Unified Communications Manager Release, versión 12.5(1)SU7 y 14SU3.
  - Cisco Unified Communications Manager IM & Presence Service Release, versión 12.5(1)SU7 y 14SU3.
  - Cisco Unified Communications Manager Session Management Edition Release versión 12.5(1)SU7 y 14SU3.
  - Cisco Unity Connection Release, versión 14SU3.
- La vulnerabilidad CVE-2023-20235 afecta a los dispositivos Cisco si ejecutan una versión vulnerable del software Cisco IOS XE, están configurados con el entorno de alojamiento de aplicaciones Cisco IOx y tienen habilitada la función de flujo de trabajo de desarrollo de aplicaciones:
  - Conmutadores resistentes Catalyst IE3x00.
  - Enrutadores resistentes Catalyst IR1100.
  - Enrutadores resistentes Catalyst IR1800.
  - Enrutadores de la serie Catalyst IR8100 de servicio pesado.
  - Enrutadores resistentes Catalyst IR8300.
  - Servicios integrados Switches serie 3300.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible lanzada por Cisco.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cer-priv-esc-B9t3hqk9 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-apidos-PGsDcdNF hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rdocker-uATbukKn

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°234	Fecha: 04-10-2023
		Página: 7 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en WordPress		
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 múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo neutralización inadecuada de elementos especiales utilizados en un comando SQL (Inyección SQL), divulgación de información y secuencia de comandos entre sitios en el complemento de publicaciones de correo electrónico a suscriptores para WordPress. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación y realizar ataques de secuencias de comandos entre sitios.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2022-46818 de tipo inyección SQL, existe debido a una limpieza insuficiente de los datos proporcionados por los usuarios. Un atacante 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.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-41735 de tipo divulgación de información, existe debido a la salida excesiva de datos por parte de la aplicación. Un atacante remoto puede obtener acceso no autorizado a información confidencial del sistema.

Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-42736.

A. Productos afectados:

- Email posts to subscribers: version 4.8 - 6.2.

3. RECOMENDACIÓN:

- Actualizar el paquete afectado con la última versión de software disponible que el proveedor lance para abordar esta vulnerabilidad, aunque aún no se conoce ninguna solución oficial.

Fuente de Información:	• hxxp://patchstack.com/database/vulnerability/email-posts-to-subscribers/wordpress-email-posts-to-subscribers-plugin-6-2-sql-injection • hxxp://patchstack.com/database/vulnerability/email-posts-to-subscribers/wordpress-email-posts-to-subscribers-plugin-6-2-sensitive-data-exposure • hxxp://patchstack.com/database/vulnerability/email-posts-to-subscribers/wordpress-email-posts-to-subscribers-plugin-6-2-cross-site-scripting-xss