	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°192	Fecha: 16-08-2023
		Página: 5 de 16

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de 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 **ALTA** de tipo escalada de privilegios, escritura de archivos arbitrarios, inyección SQL y de denegación de servicio en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto / local autenticado elevar privilegios y ejecutar comandos arbitrarios como root, generar una condición de denegación de servicio (DoS) y realizar ataques de inyección SQL.

2. DETALLES:

La vulnerabilidad de severidad **alta** registrada como CVE-2023-20224 en la interfaz de la línea de comandos (CLI) de Cisco ThousandEyes Enterprise Agent, podría permitir a un atacante local autenticado elevar privilegios a la raíz en un dispositivo afectado. Esta vulnerabilidad se debe a una validación de entrada insuficiente de los argumentos de la CLI proporcionados por el usuario. Un atacante podría explotar esta vulnerabilidad al autenticarse en un dispositivo afectado y usar comandos manipulados en el aviso. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios como root. El atacante debe tener credenciales válidas en el dispositivo afectado.

La vulnerabilidad de severidad **alta** registrada como CVE-2023-20229 en la función CryptoService de la aplicación Cisco Duo Device Health para Windows podría permitir que un atacante local autenticado con pocos privilegios realice ataques transversales de directorio y sobrescriba archivos arbitrarios en un sistema afectado. Esta vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad ejecutando un ataque transversal de directorio en un host afectado. Una explotación exitosa podría permitir que un atacante use una clave criptográfica para sobrescribir archivos arbitrarios con privilegios de nivel de SYSTEM, lo que resultaría en una condición de denegación de servicio o pérdida de datos en el sistema afectado.

La vulnerabilidad de severidad **alta** registrada como CVE-2023-20211 en la interfaz de administración basada en web de Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME) podría permitir que un atacante remoto autenticado realice ataques de inyección SQL en un sistema afectado. Esta vulnerabilidad se debe a una validación incorrecta de la entrada proporcionada por el usuario. Un atacante podría explotar esta vulnerabilidad al autenticarse en la aplicación como un usuario con privilegios de solo lectura o superiores y enviar solicitudes HTTP manipuladas a un sistema afectado. Una explotación exitosa podría permitir al atacante leer o modificar datos en la base de datos subyacente o elevar sus privilegios.

La vulnerabilidad de severidad **alta** registrada como CVE-2023-20197 en el analizador de imágenes del sistema de archivos para Hierarchical File System Plus (HFS+) de ClamAV podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado. Esta vulnerabilidad se debe a una verificación incorrecta de finalización cuando se descomprime un archivo, lo que puede generar una condición de bucle que podría hacer que el software afectado deje de responder. Un atacante podría aprovechar esta vulnerabilidad enviando una imagen del sistema de archivos HFS+ manipulada para que ClamAV la escanee en un dispositivo afectado. Una explotación exitosa podría permitir que el atacante provoque que el proceso de escaneo de ClamAV deje de responder, lo que resultaría en una condición DoS en el software afectado y consumiría los recursos disponibles del sistema.

La vulnerabilidad de severidad **alta** registrada como CVE-2023-20212 en el módulo AutoIt de ClamAV podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado. Esta vulnerabilidad se debe a un error lógico en la gestión de memoria de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad enviando un archivo AutoIt diseñado para que ClamAV lo escanee en el dispositivo afectado. Una explotación exitosa podría permitir que el atacante provoque que el proceso de escaneo de ClamAV se reinicie inesperadamente, lo que resultaría en una condición de DoS.

A. Productos afectados:

- La vulnerabilidad CVE-2023-20224 afecta la instalación del dispositivo virtual de Cisco ThousandEyes Enterprise Agent, versión 0.216 y anteriores;
- La vulnerabilidad CVE-2023-20229 afecta a la aplicación Cisco Duo Device Health (versión 4.0 y anteriores, 5.0.0, y 5.1.0) para Windows;
- La vulnerabilidad CVE-2023-20211 afecta a Cisco Unified CM y Cisco Unified CM SME (versión 11.5, 12.5 y 14);
- La vulnerabilidad CVE-2023-20197 afecta a Secure Endpoint Private Cloud y Secure Endpoint Connector para Linux, MacOS y Windows;
- La vulnerabilidad CVE-2023-20212 afecta las versiones de Secure Endpoint Connector para Windows entre la versión 8.1.5.21322 y la primera versión corregida y Secure Endpoint Private Cloud.

Asimismo, Cisco señalo que los dispositivos virtuales Cisco ThousandEyes Enterprise ejecutan un servidor Ubuntu Linux y tienen el paquete de actualizaciones desatendidas instalado de forma predeterminada, lo que garantiza que todas las correcciones de seguridad críticas se instalen automáticamente. Las actualizaciones desatendidas requieren acceso a Internet y a los repositorios de Ubuntu.

Por otro lado, la empresa indico que las versiones actualizadas de Cisco Secure Endpoint están disponibles a través del portal de Cisco Secure Endpoint. Según la política configurada, Cisco Secure Endpoint se actualizará automáticamente.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thoueye-privesc-NVhHGwb3 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-dha-filewrite-xPMBMZAK • hXXps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-injection-g6MbwH2 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-rNwNEEee • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-FTkhqMWZ