CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de Software

Fecha: **25/10/2022**

Problemática: **Vulnerabilidad en Productos Cisco**

Correlativo: **AA-0057**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

Cisco emitió un comunicado para informar a sus clientes sobe dos vulnerabilidades de seguridad en productos Cisco identificadas como CVE-2020-3433 y CVE-2020-3153. La explotación exitosa de una de estas vulnerabilidades podría permitir que un atacante local autenticado realice actividades maliciosas en el sistema objetivo.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, las vulnerabilidades afectan al canal de comunicación entre procesos (IPC) de Cisco AnyConnect Secure Mobility Client para Windows, La falla en la validación insuficiente de los recursos que carga la aplicación en tiempo de ejecución. Un atacante podría aprovechar esta vulnerabilidad enviando un mensaje IPC manipulado al proceso de AnyConnect. Una explotación exitosa podría permitir que el atacante ejecute código arbitrario en la máquina afectada con privilegios de sistema y secuestrar ficheros DLL. Para aprovechar esta vulnerabilidad, el atacante necesitaría tener credenciales válidas en el sistema Windows.

Recursos afectados:

- **Cisco AnyConnect Secure Mobility Client para Windows anteriores a la versión 4.9.00086**

RECOMENDACIONES

Actualizar la versión de Cisco AnyConnect Secure Mobility Client

- **Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación**

DICCIONARIO DE DATOS

- **Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.**
- **Fichero: Archivo diseñado para inicializar un programa (instalación, ejecución, etc.) debido a que en su interior están las instrucciones precisas para poder ejecutar un software determinado.**
- **Código arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad**

REFERENCIAS

1. **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW**
2. **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj**

ÁREA PARA DEFINICIONES