CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de Software

Fecha: 28/10/2022

Problemática: Vulnerabilidad en Productos Zoom

Correlativo: AA-0061

Institución / Sector: Instituciones Públicas y Privadas

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**

CONTEXTO

Zoom Video Comunicaciones INC emitió un comunicado para informar a sus clientes sobre una vulnerabilidad de seguridad que afecta a sus productos identificada como CVE-2022-28763. La explotación exitosa de una de estas vulnerabilidades podría permitir que un atacante local autenticado realice actividades maliciosas en el sistema objetivo.

SITUACIÓN

El cliente del software Zoom para reuniones virtuales para las plataformas Android, iOS, Linux, macOS y Windows, es susceptible a una vulnerabilidad de análisis de URL. Si se abre una URL de reunión de Zoom maliciosa, el enlace malicioso puede indicar al usuario que se conecte a una dirección de red arbitraria, lo que genera ataques adicionales, incluida la toma de control de la sesión de videoconferencia.

Recursos afectados:

Cliente Zoom para Windows: 5.0.0 23168.0427 - 5.12.0 8964

Cliente Zoom para Linux: 5.1.418436.0628 - 5.12.0 4682

Cliente Zoom para iOS: 5.0.0 23161.0427 - 5.12.0 4802

Cliente Zoom para macOS: 5.0.0 23186.0427 - 5.12.0 11129

Cliente Zoom para Android: 5.0.1 23478.0429 - 5.12.1 8902

RECOMENDACIONES

Zoom Video Comunicaciones INC recomienda a sus usuarios a que realicen la actualización del software a su nueva versión para mitigar la falla.

DICCIONARIO DE DATOS

- URL (Uniform Resource Locator): Hace referencia a la dirección que identifica un contenido colgado en Internet.
- Código arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit)

REFERENCIAS

1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW
2. https://explore.zoom.us/en/trust/security/security-bulletin/#ZSB-22024

ÁREA PARA DEFINICIONES

*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.