| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°039 | Fecha: 14-02-2024 |
|---|---|---|
| | | Página: 8 de 12 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Vulnerabilidad de ejecución remota de código en el cliente Zoom para Windows | | |
| 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 una vulnerabilidad de severidad **ALTA** de tipo error de validación de entrada en el cliente Zoom para Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema afectado.

**2. DETALLES:**

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-24691 de tipo error de validación de entrada existe debido a una validación insuficiente de la entrada proporcionada por el usuario. Un atacante remoto puede engañar a la víctima para que haga clic en un enlace especialmente diseñado y ejecute código arbitrario en el sistema.

**A. Productos afectados:**

- Zoom Client for Windows: 5.0.0 23168.0427 - 5.16.2 22807.
- Virtual Desktop Infrastructure (VDI): 5.0.1 - 5.16.0 24280.
- Zoom Meeting SDK for Windows: 5.9.0 - 5.16.2.
- Zoom Rooms for Windows: 5.0.0 1420.0426 - 5.16.10 3425.

**3. RECOMENDACIÓN:**

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

| | |
|---|---|
| Fuente de Información: | • hxxps://www.zoom.com/en/trust/security-bulletin/ZSB-24008/ |