

Vulnerabilidad Cámaras Hikvision

Fecha: 28/09/2022

Problemática: Vulnerabilidad de inyección de comando de cámaras IP de Hikvision

Correlativo: AA-0025

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

De acuerdo al reporte emitido por el Centro de respuesta de seguridad de Hikvision (HSRC) desarrolladora de tecnologías de sensores IoT, informo en medios oficiales sobre una vulnerabilidad identificada como CVE-2021-36260 (versión anterior CVE-2021-210628) que afecta a una gama de ciertos de sus productos.

SITUACIÓN

La vulnerabilidad descubierta permite la ejecución remota de código no autenticado (RCE) en el firmware de la cámara IP/NVR de Hikvision, lo que da lugar a una inyección de comandos en el servidor web.

Debido a la validación de entrada insuficiente, un ciberdelincuente puede aprovechar la vulnerabilidad para lanzar un ataque de inyección de comandos mediante el envío de mensajes manipulados con comandos maliciosos.

Nivel de priorización

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

Matriz de Evaluación

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

RECOMENDACIONES

Verificar la versión del firmware instalado en el dispositivo, si la misma es anterior a la 210628. Instale las actualizaciones de inmediato.

Información de versiones afectadas y versiones resueltas:
<https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/security-notification-command-injection-vulnerability-in-some-hikvision-products/>

DICCIONARIO DE DATOS

1. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
2. Código Arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
3. Internet de las cosas (IoT): describe la red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet.

REFERENCIAS

1. Alerta Hikvision

<https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/>

2. <https://nvd.nist.gov/vuln/detail/CVE-2021-36260>

3. <https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html>

ÁREA PARA DEFINICIONES