

Vulnerabilidad Cámaras Hikvision

Fecha: 07/09/2022

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

Correlativo: AA-0022

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

Matriz de Evaluación

Prioridad Urgente / No Urgente		Actualización Seguimiento/Preventiva/Resiliente		
Urgente		Preventiva		
Riesgo Alto/ Medio/ Bajo	Integridad	Nivel de Afectación		
		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

- Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
- 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.
- 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

- Alerta Hikvision <https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/>
- <https://nvd.nist.gov/vuln/detail/CVE-2021-36260>
- <https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html>

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 bórralo 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.

*La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.