BOLETÍN DE ALERTA

Boletín Nro.: 2021-28

Fecha de publicación: 28/09/2021

Tema: Vulnerabilidad crítica en productos Hikvision.

Productos afectados:

- Cámaras Hikvision de la serie:
  - DS-2CVx, HWI-x, IPC-x, DS-2CDx, iDS-2x, DS-2Xx, PTZ-Nx, iDS-2VSx versiones de firmware anteriores a 210625
  - DS-2TDx versiones de firmware anteriores a 210702
  - DS-76x, DS-71x, DS-HiLookI-NVR-1x, DS-HiLookI-NVR-2x con las versiones de firmware anteriores a 210511
- NVR Hikvision de la serie:
  - DS-HiLookI-NVR-1x, DS-HiLookI-NVR-2x con las versiones de firmware anteriores a 210511

Para ver la lista detallada de los productos afectados ingrese al siguiente enlace: Notificación de Seguridad Hikvision.

Descripción:

Una vulnerabilidad crítica identificada como CVE-2021-36260, afecta al firmware de las cámaras IP de Hikvision, tanto a los firmwares más recientes (al 21 de junio de 2021), como también otros más antiguos desde al menos el año 2016. Esta vulnerabilidad no solo afecta a cámaras IP, sino que también está presente en algunos modelos de NVR. La vulnerabilidad se debe a una validación de entrada insuficiente y puede explotarse enviando mensajes especialmente diseñados a dispositivos vulnerables.

Un actor malintencionado podría obtener el control total del dispositivo simplemente con un Shell raíz sin acceso de administrador. Según indican los investigadores, incluso podrían tener más permisos que los propios propietarios del dispositivo, ya que están restringidos a un Shell protegido limitado.

El atacante únicamente necesitaría acceso al puerto del servidor HTTPS, que generalmente suele ser 80/443. No se requeriría nombre de usuario, ni contraseña. Además, el propietario de la cámara no tendría que realizar ninguna acción y todo el proceso sería indetectable.

Por su forma de ejecución y el control que puede tomar un hipotético atacante, ha obtenido una puntuación de 9,8 que la convierte en una vulnerabilidad de severidad crítica.

Impacto:

La explotación exitosa de la vulnerabilidad podría permitir a un atacante ejecutar código remoto (RCE) y obtener el control total del sistema.

Solución:

Instalar las actualizaciones del fabricante disponibles en los medios oficiales del proveedor: https://www.hikvision.com/es-la/support/download/firmware1/

En el caso de que no pueda actualizar el firmware del sistema afectado debe adoptar medidas de mitigación temporal tal como despublicar y/o restringir el acceso al servicio de administración web desde Internet.

Información adicional:

- https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html
- https://www.hikvision.com/es-la/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/security-notification-command-injection-vulnerability-in-some-hikvision-products/
- https://us-cert.cisa.gov/ncas/current-activity/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260