Se han compartido los detalles de una vulnerabilidad de seguridad en la implementación estándar del Open Network Video Interface Forum (ONVIF) de Dahua, que al ser explotada, puede llevar a tomar el control de las cámaras IP.

Rastreada como CVE-2022-30563 (puntaje CVSS: 7.4), *«los atacantes podrían abusar de la vulnerabilidad para comprometer las cámaras de red olfateando una interacción ONVIF anterior sin cifrar y reproduciendo las credenciales en una nueva solicitud hacia la cámara»*, dijo Nozomi Networks.

El problema, que se solucionó en un parche publicado el 28 de junio de 2022, afecta a los siguientes productos:

- Dahua ASI7XXX: Versiones anteriores a v1.000.0000009.0.R.220620
- Dahua IPC-HDBW2XXX: Versiones anteriores a v2.820.0000000.48.R.220614
- Dahua IPC-HX2XXX: Versiones anteriores a v2.820.0000000.48.R.220614

ONVIF rige el desarrollo y el uso de un estándar abierto sobre cómo los productos de seguridad física basados en IP, como las cámaras de videovigilancia y los sistemas de control de acceso, pueden comunicarse entre sí de forma independiente del proveedor.

El error identificado por Nozomi Networks reside en lo que se llama el mecanismo de autenticación «WS-UsernameToken» implementado en ciertas cámaras IP desarrolladas por la compañía china Dahua, lo que permite a los atacantes comprometer las cámaras reproduciendo las credenciales.

Dicho de otra forma, la explotación exitosa de la vulnerabilidad podría permitir que un adversario agregue de forma encubierta una cuenta de administrador malicioso y la explote para obtener acceso sin restricciones a un dispositivo afectado con los privilegios más altos, incluida la visualización de transmisiones de cámaras en vivo.

Todo lo que un actor de amenazas necesita para montar este ataque es poder capturar una solicitud ONVIF sin cifrar autenticada con el esquema WS-UsernameToken, que luego se

utiliza para enviar una solicitud falsificada con los mismos datos de autenticación para engañar al dispositivo para que cree la cuenta de administrador.

Esta divulgación sigue al descubrimiento de fallas similares en los dispositivos Reolink, ThrougTek, Annke y Axis, lo que subraya los riesgos potenciales que plantean los sistemas de cámaras de seguridad IoT debido a su implementación en instalaciones de infraestructura crítica.

> *«Los actores de amenazas, en particular los grupos de amenazas de los estados nacionales, podrían estar interesados en hackear cámaras IP para ayudar a recopilar información sobre el equipo o los procesos de producción de la empresa objetivo»,* dijeron los investigadores.

> *«Esta información podría ayudar en el reconocimiento realizado antes de lanzar un ataque cibernético. Con más conocimiento del entorno objetivo, los actores de amenazas podrían crear ataques personalizados que pueden interrumpir físicamente los procesos de producción en la infraestructura crítica».*

En un desarrollo relacionado, los investigadores de NCC Group documentaron 11 vulnerabilidades que afectan a los procesos de cerraduras inteligentes de Nuki, que podrían armarse para obtener ejecución de código arbitrario y abrir puertas o causar una condición de denegación de servicio (DoS).

También es notable un aviso del sistema de control industrial (ICS) emitido por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos esta semana, que advierte sobre dos vulnerabilidades de seguridad graves en los servidores MOXA NPort 5110 que ejecutan la versión de firmware 2.10.

> *«La explotación exitosa de estas vulnerabilidades podría permitir que un atacante cambie los valores de la memoria y/o haga que el dispositivo deje de responder»,* dijo la agencia.