Las vulnerabilidades de seguridad recién descubiertas en las cámaras de seguridad domésticas Blue (antes LifeShield) de ADT, podrían haberse aprovechado para secuestrar transmisiones de audio y video.

Las vulnerabilidades, rastreadas como CVE-2020-8101, fueron identificadas en la cámara del timbre de video por los investigadores de Bitdefender en febrero de 2020 antes de que finalmente se abordaran el 17 de agosto de 2020.

LifeShield fue adquirida por ADT Inc. con sede en Florida en 2019, y las soluciones de seguridad para el hogar de Lifeshield se rebautizaron como Blue a partir de enero de 2020. Los productos de la compañía tuvieron una participación de mercado del 33.6% en Estados Unidos el año pasado.

Los problemas de seguridad en la cámara del timbre permiten que un atacante haga lo siguiente:

- Obtener la contraseña de administrador de la cámara simplemente conociendo su dirección MAC, que se utiliza para identificar un dispositivo de forma única
- Inyectar comandos localmente para obtener acceso de root
- Acceder a las fuentes de audio y video mediante un servidor RTSP (Protocolo de transmisión en tiempo real) sin protección

El timbre está diseñado para enviar de forma periódica mensajes de latido a *«cms.lifeshield.com»,* que contienen información como la dirección MAC, SSID, dirección IP local y la intensidad de la señal inalámbrica. El servidor, a cambio, responde con un mensaje de autenticación que se puede eludir trivialmente creando una solicitud falsa utilizando la dirección MAC del dispositivo.

> *«El servidor parece ignorar el token y verifica solo la dirección MAC cuando envía una respuesta. La contraseña del administrador se puede obtener decodificando el encabezado de autorización base64 recibido en esta solicitud»,* dijeron los

> investigadores.

Armado con este acceso de administrador a la interfaz web de la cámara, el atacante puede aprovechar una interfaz HTTP que es vulnerable a la inyección de comandos y obtener acceso de root.

Finalmente, los investigadores encontraron que un servidor RTSP no seguro sin credenciales podría explotarse para acceder al flujo de video en *«rtsp://10.0.0.108:554/img/media.sav»* usando cuando reproductor multimedia.

Aunque se han aplicado parches a los servidores de producción y a los 1500 dispositivos afectados, sin una forma simple de confirmar si los usuarios de la cámara instalaron las actualizaciones de firmware, Bitdefender decidió retrasar la divulgación pública en más de cinco meses.

> *«Los clientes tienen opciones de seguridad cuando se trata de proteger sus hogares inteligentes o pequeñas empresas. Investigar cuidadosamente a los proveedores de IoT para las políticas de actualización de seguridad para sus productos, cambiar las contraseñas predeterminadas, separar los IoT en diferentes subredes e incluso verificar regularmente las actualizaciones de firmware son solo algunos consejos prácticos de seguridad que cualquiera puede cumplir»*, dijeron los investigadores.