Expertos en seguridad cibernética publicaron hoy un informe advirtiendo que la nueva y creciente tecnología LoRaWAN, es vulnerable a ataques cibernéticos y configuraciones erróneas, a pesar de las afirmaciones de seguridad mejorada sobre el uso del protocolo de dos capas de cifrado.

LoRaWAN, que significa *«Red de Área Amplia de Largo Alcance»,* es una tecnología basada en radio que funciona por encima del protocolo patentado LoRa.

El protocolo LoRa se desarrolló para permitir a las compañías conectar a Internet dispositivos con batería u otros dispositivos de baja potencia por medio de una conexión inalámbrica.

LoRaWAN adopta el protocolo LoRa y permite que los dispositivos distribuidos en una gran área geográfica se puedan conectar de forma inalámbrica a Internet por medio de ondas de radio.

Antes, para conectar un IoT o cualquier otro dispositivo inteligente a Internet, las compañías tenían que conectar el dispositivo IoT a su red WiFi privada de Internet o los dispositivos tenían que enviarse con una tarjeta SIM, lo que permitía que el dispositivo utilizara una red celular para informar a un servidor de comando.

LoRaWAN es una alternativa a esas configuraciones. Un dispositivo IoT con un cliente LoRaWAN transmitirá datos por medio de ondas de radio a una puerta de enlace LoRaWAN cercana, en la mayoría de los casos, una antena. El Gateway toma estos datos y los reenvía a un servidor de Internet, que luego los transmite a un backend o tablero de aplicaciones.

Este tipo de configuraciones de LoRaWAN se usa por lo general en el mundo real. Por ejemplo, el estacionamiento inteligente, la iluminación inteligente, gestión del tráfico o los dispositivos de monitoreo del clima en una *«ciudad inteligente»*, utilizan LoRaWAN para informar a una estación central de recolección de datos.

Debido a que el protocolo funciona a través de ondas de radio en lugar de depender de las redes WiFi o tarjetas SIM, esto hace que las configuraciones complejas de IoT sean más

fáciles de implementar, ya que es más fácil instalar algunas antenas de radio en un área geográfica pequeña en comparación con decenas de enrutadores WiFi o miles de tarjetas SIM.

Gracias a este enfoque de bajo costo, las redes LoRaWAN también se utilizan a menudo en instalaciones industriales (para informar lecturas de distintos sensores o equipos SCADA), hogares inteligentes, hospitales inteligentes, campos de cultivo inteligentes, etcétera.

Pero transmitir datos desde dispositivos por medio de ondas de radio no es un enfoque seguro. Sin embargo, los desarrolladores del protocolo anticiparon dicho problema. Desde su primera versión, LoRaWAN ha utilizado dos capas de cifrado de 128 bits para proteger los datos que se transmiten desde los dispositivos, con una clave de cifrado utilizada para autenticar el dispositivo contra el servidor de red y el otro contra la aplicación de fondo de una empresa.

En un informe publicado hoy, los investigadores de seguridad de IOActive, afirman que el protocolo es propenso a configuraciones erróneas y opciones de diseño que lo hacen susceptible a piratería informática y ataques cibernéticos.

La compañía enumeró distintos escenarios que encontraron plausibles durante su análisis del protocolo de rápido crecimiento:

- Las claves de cifrado se pueden extraer de los dispositivos mediante ingeniería inversa del firmware de los dispositivos que se envían con un módulo LoRaWAN.
- Muchos dispositivos cuentan con una etiqueta que muestra un código QR o texto con el identificador del dispositivo, incluyendo claves de seguridad.
- Los investigadores dicen que la etiqueta está destinada a ser utilizada en el proceso de puesta en marcha y eliminada después.
- Algunos dispositivos pueden incluir claves de cifrado codificadas que se envían con algunas bibliotecas LoRaWAN de código abierto (destinadas a ser reemplazadas antes de implementarse en el dispositivo).

- Algunos dispositivos pueden utilizar claves de cifrado fáciles de adivinar, como AppKey = identificador de dispositivo + identificador de aplicación, o también, AppKey = identificador de aplicación + identificador del dispositivo.
- Los servidores de red LoRaWAN pueden estar configurados de forma insegura o son vulnerables a otras vulnerabilidad que no sean LoRaWAN, lo que permite a hackers tomar el control de los sistemas.
- Las vulnerabilidades en el diseño del protocolo permiten ataques de denegación de servicio.

> *«Las organizaciones confían ciegamente en LoRaWAN porque está cifrado, pero ese cifrado se puede pasar por alto fácilmente si los hackers pueden tener acceso a las teclas, lo que nuestra investigación muestra que pueden hacer de distintas formas, con relativa facilidad»,* dijo Cesar Cerrudo, director de tecnología de IOActive.
>
> *«Una vez que los piratas informáticos tienen acceso, existen muchas cosas que podrían hacer: podrían evitar que las empresas de servicios públicos tomen lecturas de medidores inteligentes, impedir que las empresas de logística rastreen vehículos o prohibir que los hospitales reciban lecturas de equipos inteligentes. En casos extremos, una red comprometida podría alimentarse con lecturas falsas del dispositivo para ocultar ataques físicos contra la infraestructura, como una tubería de gas. O para provocar que un equipo industrial que contiene sustancias volátiles se corrija en exceso, causando que se rompa, queme o incluso explote»,* agregó.

Para evitar implementaciones inseguras de redes LoRaWAN, los investigadores de IOActive recomiendan auditar dispositivos y redes LoRaWAN, pero también se deben implementar medidas de seguridad adicionales como el monitoreo del tráfico LoRaWAN, de forma similar a cómo las compañías tratarían el tráfico web HTTP/HTTPS normal.

Con el fin de ayudar en parte de la auditoría, la compañía lanzó en GitHub un marco de auditoría de código abierto LoRaWAN llamado LAF.