Una vulnerabilidad grave reside en el protocolo central que se encuentra en la gran mayoría de los dispositivos de Internet de las Cosas (IoT).

La vulnerabilidad, denominada como CallStranger, permite a los hackers secuestrar dispositivos inteligentes para realizar ataques distribuidos de denegación de servicio (DDoS), pero también para ataques que omiten soluciones de seguridad para alcanzar y realizar exploraciones en la red interna de la víctima, otorgando efectivamente a los atacantes acceso a áreas donde normalmente no podrían alcanzar.

Según el sitio web dedicado de CallStranger publicado hoy, el error afecta a UPnP, que significa Universal Plug and Play, una colección de protocolos que se envían en la mayoría de dispositivos inteligentes.

La función UPnP permite que los dispositivos se vean en las redes locales y después establezcan conexiones para intercambiar de forma sencilla los datos, configuraciones e incluso trabajar en sincronización.

UPnP ha existido desde el año 2000 aproximadamente, pero desde 2016, su desarrollo ha sido administrado por la Open Connectivity Foundation (OCF), que controla los protocolos UPnP, en un esfuerzo por estandarizar el funcionamiento de estas características en todos los dispositivos.

En diciembre de 2019, un ingeniero de seguridad llamado Yunus Cadirci, encontró un error en esta tecnología tan extendida. El investigador asegura que un atacante puede enviar paquetes TCP a un dispositivo remoto que contiene un valor de encabezado de devolución de llamada mal formado en la función SUSCRIBIRSE de UPnP.

Se puede abusar el encabezado mal formado para aprovechar cualquier dispositivo inteligente que se conecte a Internet y que admita los protocolos UPnP, como cámaras de seguridad, DVR, impresoras, enrutadores, entre otros.

En un ataque CallStranger, el hacker se dirige efectivamente a la interfaz de Internet del

dispositivo, pero ejecuta el código en la función UPnP del dispositivo, que generalmente se ejecuta solo en los puertos internos.

Cadirci afirma que los atacantes podrían usar el error CallStranger para evitar las soluciones de seguridad de la red, omitir los firewalls y escanear las redes internas de una empresa.

El investigador dijo que notificó a la OCF el año pasado y la organización ha actualizado los protocolos UPnP desde su informe. Las actualizaciones de los protocolos UPnP se lanzaron el 17 de abril de 2020, y el equipo de CERT/CC dice que algunos proveedores pueden tardar en aplicar las actualizaciones.

> *«Debido a que esta es una vulnerabilidad de protocolo, los proveedores pueden tardar mucho tiempo en proporcionar parches»*, dijo Cadirci hoy.

Asimismo, el investigador publicó hoy un sitio web con consejos básicos que las empresas pueden implementar para bloquear cualquier intento de explotación.

También publicó scripts de prueba de concepto que las compañías pueden utilizar para determinar si un dispositivo inteligente es vulnerable a cualquiera de los ataques CallStranger.

CallStranger se rastrea como CVE-2020-12695. Actualmente existen aproximadamente 5.45 millones de dispositivos con capacidad UPnP conectados a Internet, lo que significa una superficie de ataque ideal para botnets y APT de IoT.