FACUA.org - Internacional - 3 de enero de 2019

Una vulnerabilidad en los Chromecast permite ejecutar comandos de voz maliciosos mediante Amazon Echo

Una vulnerabilidad presente en los dispositivos Chromecast permite utilizar el asistente digital Amazon Alexa y los altavoces inteligentes Echo de la compañía para ejecutar comandos de voz maliciosos en los dispositivos domésticos conectados.

Según ha advertido la compañía de ciberseguridad Pen Test Partners, aunque los altavoces Amazon Echo no pueden hackearse directamente, es posible aprovechar las brechas de seguridad de otros dispositivos conectados para ejecutar comandos de voz a distancia a través de Echo y Alexa.

La vulnerabilidad se encuentra presente en los Chromecast, utilizados para lanzar contenido a televisores no compatibles, y aunque se detectó por primera vez en 2014 continúa activa en las últimas versiones del dispositivos.

Según la compañía de seguridad, este problema se puede encontrar también en modelos antiguos de televisores inteligentes de varios fabricantes entre los que se encuentran Samsung y Sony.

A través de distintos mecanismos entre los que se incluye la obtención de las claves WiFi de los *router* domésticos con baja seguridad, la compañía de seguridad utilizó la vulnerabilidad de Chromecast para ejecutar comandos de voz en otros dispositivos domésticos.

Entre los dispositivos del Internet de las Cosas afectados por esta vulnerabilidad se encuentran sistemas de luz, televisores, alarmas y electrodomésticos como hervidores de agua. También resulta posible efectuar compras por comandos de voz desde Amazon si el cliente afectado tiene activada la opción de compras en un clic.