Investigadores de seguridad cibernética revelaron una vulnerabilidad de seguridad sin parches, que podría representar un riesgo grave para los productos de IoT.

La vulnerabilidad, que se informó originalmente en septiembre de 2021, afecta la implementación del Sistema de Nombres de Dominio (DNS) de dos bibliotecas C populares llamadas uClibc y uClibc-ng que se utilizan para desarrollar sistemas Linux integrados.

Se sabe que uClibc es utilizada por los principales proveedores como Linksys, Netgear y Axis, así como por distribuciones de Linux como Embedded Gentoo, lo que podría exponer millones de dispositivos IoT a amenazas de seguridad.

> *«La falla es causada por la previsibilidad de los ID de transacción incluidos en las solicitudes de DNS generadas por la biblioteca, lo que puede permitir a los atacantes realizar ataques de envenenamiento de DNS contra el dispositivo de destino»,* dijeron Giannis Tsaraias y Andrea Palanca, de Nozomi Networks.

El envenenamiento de DNS, también conocido como falsificación de DNS, es la técnica de corromper un caché de resolución de DNS, que proporciona a los clientes la dirección IP asociada con un nombre de dominio, con el objetivo de redirigir a los usuarios a sitios web maliciosos.

La explotación exitosa del error podría permitir que un adversario realice ataques Man-in-the-Middle (MitM) y corrompa el caché de DNS, redirigiendo efectivamente el tráfico de Internet a un servidor bajo su control.

Nozomi Networks advirtió que la vulnerabilidad podría explotarse trivialmente de forma confiable si el sistema operativo se configura para usar un puerto de origen fijo o predecible.

> *«El atacante podría entonces robar y/o manipular la información transmitida por los usuarios y realizar otros ataques contra esos dispositivos para comprometerlos*

> *completamente»,* dijeron los investigadores.