Un grupo de académicos de la Universidad de California y la Universidad de Tsinghua descubrió una serie de fallas de seguridad críticas que podrían conducir a una reactivación de los ataques de envenenamiento de caché de DNS.

Nombrada como SAD DNS Attack (Abreviatura de Side-channel AttackeD DNS), la técnica hace posible que un actor malintencionado lleve a cabo un ataque fuera de ruta, redireccionando cualquier tráfico originalmente destinado a un dominio específico a un servidor bajo su control, lo que les permite espiar y manipular las comunicaciones.

> *«Esto representa un hito importante: el primer ataque de canal lateral de red armable que tiene graves impactos en la seguridad. El ataque permite que un hacker fuera de ruta inyecte un registro DNS malicioso en una caché de DNS»,* dijeron los investigadores.

Con el seguimiento de CVE-2020-25705, los hallazgos se presentaron en la Conferencia ACM sobre seguridad informática y de comunicaciones (CCS ’20) celebrada esta semana.

La falla afecta a los sistemas operativos Linux 3.18-5.10, Windows Server 2019 (versión 1809) y posteriores, macOS 10.15 y posteriores, y FreeBSD 12.1.0 y posteriores.

Los solucionadores DNS por lo general almacenan en caché las respuestas a las consultas de direcciones IP durante un período específico como un medio para mejorar el rendimiento de la respuesta en una red. Pero este mismo mecanismo puede explotarse para envenenar los cachés haciéndose pasar por las entradas de DNS de la dirección IP de un sitio web determinado y redirigir a los usuarios que intentan visitar ese sitio web a otro sitio que elija el atacante.

Sin embargo, la efectividad de dichos ataques se ha visto afectada en parte debido a

protocolos como DNSSEC (Extensiones de seguridad del sistema de nombres de dominio), que crean un sistema de nombres de dominio seguro al agregar firmas criptográficas a los registros DNS existentes y defensas basadas en la aleatorización que permiten al DNS resolver para usar un puerto de origen y un ID de transacción (TxID) distintos para cada consulta.

Los investigadores señalan que las dos medidas de mitigación aún están lejos de ser ampliamente implementadas por razones de *«incentivos y compatibilidad»*, por lo que idearon un ataque de canal lateral que se puede usar con éxito contra las pilas de software DNS más populares, lo que hace que los resolutores de DNS públicos como el 1.1.1.1 de Cloudflare y el 8.8.8.8 de Google sean vulnerables.

Nuevo ataque de canal lateral

El ataque SAD DNS funciona mediante el uso de una máquina comprometida en cualquier red que sea capaz de desencadenar una solicitud de un reenviador o resolutor de DNS, como una red inalámbrica pública administrada por un enrutador inalámbrico en una cafetería, un centro comercial o un aeropuerto.

Después, aprovecha un canal lateral en la pila de protocolos de red para escanear y descubrir qué puertos de origen se utilizan para iniciar una consulta de DNS y posteriormente, inyectar una gran cantidad de respuestas de DNS falsificadas mediante la fuerza bruta de los TxID.

Los investigadores utilizaron un canal usado en las solicitudes de nombre de dominio para reducir el número de puerto de origen exacto mediante el envío de paquetes UDP falsificados, cada uno con diferentes direcciones IP, a un servidor de la víctima e inferir si las sondas falsificadas llegaron al puerto de origen correcto basado en las respuestas ICMP recibidas.

Este método de escaneo de puertos alcanza una velocidad de escaneo de 1000 puertos por segundo, lo que lleva acumulativamente un poco más de 60 segundos para enumerar todo el rango de puertos que consta de 65536 puertos. Con el puerto de origen desaleatorizado, todo lo que un atacante debe hacer es insertar una dirección IP maliciosa para redirigir el tráfico del sitio web y realizar con éxito un ataque de envenenamiento de la caché de DNS.

Además de demostrar formas de extender la ventana de ataque que permite a un atacante escanear más puertos y también inyectar registros fraudulentos adicionales para envenenar la caché de DNS, el estudio encontró que más del 34% de los resolutores abiertos en Internet son vulnerables, 85% de los cuales forman parte de servicios DNS populares como Google y Cloudflare.

Para contrarrestar el SAD DNS, los investigadores recomiendan deshabilitar las respuestas ICMP salientes y configurar el tiempo de espera de las consultas de DNS de forma más agresiva.

Además, los investigadores crearon una herramienta para buscar servidores DNS que sean vulnerables al ataque. El grupo trabajó con el equipo de seguridad del kernel de Linux para un parche que aleatoriza el límite de velocidad global ICMP para introducir ruidos en el canal lateral.

> *«La investigación presenta un canal lateral novedoso y general basado en el límite de velocidad ICMP global, implementado universalmente por todos los sistemas operativos modernos. Esto permite escaneos eficientes de puertos de origen UDP en consultas DNS. Combinado con técnicas para extender la ventana de ataque, conduce a una poderosa reactivación del ataque de envenenamiento de caché DNS»,* agregaron los investigadores.