El Internet Systems Consortium (ISC) ha lanzado actualizaciones para corregir varias vulnerabilidades de seguridad en el software del sistema de nombres de dominio (DNS) Berkeley Internet Name Domain (BIND) 9, que podrían ser explotadas para causar una condición de denegación de servicio (DoS).

> *«Un actor de amenazas cibernéticas podría explotar una de estas vulnerabilidades para provocar una condición de denegación de servicio»*, afirmó la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) en un aviso.

Las cuatro vulnerabilidades son las siguientes:

- CVE-2024-4076 (puntuación CVSS: 7.5): debido a un error lógico, las búsquedas que activaban el servicio de datos obsoletos y requerían búsquedas en datos de zona autorizada local podrían haber causado una falla de aserción.
- CVE-2024-1975 (puntuación CVSS: 7.5): la validación de mensajes DNS firmados usando el protocolo SIG(0) podría generar una carga excesiva de la CPU, resultando en una condición de denegación de servicio.
- CVE-2024-1737 (puntuación CVSS: 7.5): es posible crear un número excesivamente grande de tipos de registros de recursos para un nombre de propietario específico, lo que ralentiza el procesamiento de la base de datos.
- CVE-2024-0760 (puntuación CVSS: 7.5): un cliente DNS malicioso que envía muchas consultas a través de TCP pero nunca lee las respuestas podría hacer que el servidor responda lentamente o no responda en absoluto para otros clientes.

La explotación exitosa de estos errores podría causar que una instancia de *named* termine inesperadamente, agote los recursos de CPU disponibles, ralentice el procesamiento de consultas en un factor de 100 y haga que el servidor no responda.

Los problemas se han solucionado en las versiones BIND 9 9.18.28, 9.20.0 y 9.18.28-S1, lanzadas a principios de este mes. No hay evidencia de que estas vulnerabilidades hayan sido explotadas en la práctica.

Esta divulgación se produce meses después de que el ISC resolviera otra vulnerabilidad en BIND 9 denominada KeyTrap (CVE-2023-50387, puntuación CVSS: 7.5) que podría ser utilizada para agotar los recursos de CPU y detener los resolutores de DNS, causando una condición de denegación de servicio (DoS).