El Consorcio de Sistemas de Internet (ISC) lanzó parches para abordar múltiples vulnerabilidades de seguridad en el paquete de software del Sistema de Nombres de Dominio (DNS) de Berkeley Internet Name Domain 9 (BIND), que podría conducir a una condición de denegación de servicio (DoS).

> *«Un atacante remoto podría explotar estas vulnerabilidades para causar condiciones de denegación de servicio y fallas del sistema»*, dijo la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) en un aviso publicado el viernes.

El software de código abierto es utilizado por las principales compañías financieras, operadores nacionales e internacionales, proveedores de servicios de Internet (ISP), minoristas, fabricantes, instituciones educativas y entidades gubernamentales, según su sitio web.

Las cuatro vulnerabilidades residen en named, un servicio BIND9 que funciona como un servidor de nombres autorizado para un conjunto fijo de zonas DNS o como un solucionador recursivo para clientes en una red local.

La lista de errores, que tiene una calificación de 7.5 en el sistema de puntuación CVSS, es la siguiente:

- CVE-2022-3094: Una inundación de mensajes de ACTUALIZACIÓN puede hacer que named agote toda la memoria disponible
- CVE-2022-3488: La edición de vista previa compatible con BIND nombrada puede terminar inesperadamente al procesar opcions de ECS en respuestas repetidas a consultas iterativas
- CVE-2022-3736: El nombre configurado para responder desde la caché obsoleta puede terminar inesperadamente mientras se procesan las consultas RRSIG
- CVE-2022-3924: El nombre configurado para responder desde la memoria caché obsoleta puede terminar inesperadamente en la cuota blanda de clientes recurivos

La explotación exitosa de las vulnerabilidades podría provocar que el servicio mencionado se bloquee o agote la memoria disponible en un servidor de destino.

Los problemas afectan a las versiones 9.16.0 a 9.16.36, 9.18.0 a 9.18.10, 9.19.0 a 9.19.8 y 9.16.8-S1 a 9.16.36-S1. CVE-2022-3488 también afecta las versiones 9.11.4-S1 a 9.11.37-S1 de BIND Supported Preview Edition. Se han resuelto en las versiones 9.16.37, 9.18.11, 9.19.9 y 9.16.37-S1.

Aunque no hay evidencia de que alguna de estas vulnerabilidades esté siendo explotada activamente, se recomienda a los usuarios que actualicen a la última versión lo antes posible para mitigar las posibles amenazas.