Boletín de alerta

Boletín Nro.:
Fecha de publicación: 03/11/2025
Tema: Alerta 2025-96 Vulnerabilidad en BIND9 DNS
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- BIND versiones 9.18.41, 9.20.15, y 9.21.14

Descripción

Una vulnerabilidad de alta gravedad conocida como CVE-2025-40778 (Score 8.6) afecta a los servidores DNS (Domain Name System) mediante el ampliamente utilizado software BIND9, la cual podría ser aprovechada por atacantes remotos no autenticados para manipular entradas de nombres de dominio a través del envenenamiento de caché, permitiéndoles redirigir el tráfico de Internet hacia sitios potencialmente maliciosos, distribuir malware o interceptar las comunicaciones de red.

Al procesar las respuestas, el resolver no validó que los conjuntos de registros (RRsets) de la sección de respuesta coincidieran con la consulta (QNAME, QTYPE y QCLASS) que se estaba resolviendo. La lógica vulnerable permite que se inserten en caché registros A o CNAME adicionales incluidos en la sección de respuesta, incluso si corresponden a un nombre diferente. Esto invalida la suposición de que los atacantes

fuera de la ruta deben ganar una carrera por la tupla exacta solicitada y permite la inyección de nombres de host arbitrarios una vez que se falsifica una sola consulta de subdominio.

En la compilación probada (lib/ns/query.c y lib/dns/resolver.c de la versión 9.18.39), los registros de respuesta no solicitados sobreviven al procesamiento de la respuesta y se almacenan en caché con un TTL completo. Las versiones corregidas añaden un filtrado más estricto que descarta los RRsets que no coinciden antes de almacenarlos en caché.

Los atacantes pueden usarlo para inyectar registros falsificados (es decir, asignaciones de IP a dominio) en el caché durante una consulta y, por lo tanto, afectar potencialmente la resolución de consultas futuras y redirigir a los usuarios a recursos controlados por el atacante.

Solución:

El proveedor lanzó parches que solucionan dicha vulnerabilidad: versiones parcheadas: 9.18.41, 9.20.15, 9.21.14 (y las compilaciones correspondientes de la Edición de Vista Previa Compatible).

Información adicional:

- https://cyberpress.org/706000-bind-9-poc-released/
- https://nvd.nist.gov/vuln/detail/CVE-2025-40778
- https://www.helpnetsecurity.com/2025/10/28/bind-9-vulnerability-cve-2025-40778-poc/