Investigadores de Cisco Talos descubrieron una vulnerabilidad de denegación de servicio en el servidor BIND de Internet Systems Consortium, que existe cuando se procesa el tráfico TCP a través de la biblioteca libuv.

Un atacante puede aprovechar la vulnerabilidad al inundar el puerto TCP y forzando la terminación del servicio.

El servidor de nombres BIND se considera la implementación de referencia del sistema de nombres de dominio de Internet. Es capaz de ser un servidor de nombres autorizado así como un caché recursivo para consultas de nombres de dominio en una red. Esta vulnerabilidad solo se aplica a este código específico y no afecta a ningún otro software de DNS.

Según Cisco Talos, los investigadores trabajaron con ISC para garantizar la resolución del problema y emitir las actualizaciones necesarias para los clientes afectados.

La vulnerabilidad, rastreada como CVE-2020-8620, reside en una falla de aserción dentro del servidor BIND de Internet Systems Consortium, versiones 9.16.1 a 9.17.1, cuando se procesa el tráfico TCP a través de la biblioteca libuv.

Debido a una longitud especificada en una devolución de llamada para la biblioteca, la inundación del puerto TCP del servidor utilizado para solicitudes de DNS más grandes (AXFR), puede hacer que la biblioteca libuv pase una longitud al servidor que violará una comprobación de aserción en las verificaciones del servidor.

Esta verificación de afirmación terminará el servicio, lo que resultará en una condición de denegación de servicio. Un hacker puede inundar el puerto con paquetes no autenticados para explotar la vulnerabilidad.

> *«Una vez que el servidor ha inicializado a cada trabajador y vinculado a los puertos configurados, el servidor debe utilizar libuv para asignar una devolución de llamada*

> *a la que enviar cuando recibe una conexión en un puerto. La devolución de llamada que se utiliza para procesar TCP es la siguiente fucnión: dnslisten_acceptcb. Después de realizar algunas validaciones, llamará a la función isc_nm_read con una devolución de llamada, dnslisten_readcb, como segundo parámetro. Esta devolución de llamada se almacenará en una estructura y luego se pasará a libuv para informar a la biblioteca a qué llamar cuando el servidor necesite leer datos de un cliente TCP»*, dijo el investigador Emanuel Almeida, de Cisco Systems.

Según el investigador, para utilizar la prueba de concepto, primero se debe cambiar las variables DST_IP y DST_PORT para que apunten al host en el que está escuchando el daemon BIND y luego ejecutarlo con Python 2.x.

El proveedor lanzó el parche para corregir la vulnerabilidad el pasado 4 de agosto de 2020.