BOLETÍN DE ALERTA

Boletín Nro.: 2020-19
Fecha de publicación: 19/06/2020
Tema: Vulnerabilidades de riesgo medio, en ISC BIND permitirían a un atacante realizar ataques DoS

Producto afectado:

- BIND

Descripción:

ISC (Internet Systems Consortium) ha lanzado un aviso de seguridad que aborda **dos vulnerabilidades**, catalogadas con **riesgo medio,** que afectan a múltiples versiones de **BIND (Berkeley Internet Name Domain)**. (Software de nombres de dominio).

Estos fallos han sido identificados como **CVE-2020-8618**, que afecta a BIND a 9.16.0 a 9.16.3. Y el **CVE-2020-8619**, que afecta a BIND en sus versiones:

- 9.11.14 a 9.11.19,
- 9.14.9 a 9.14.12,
- 9.16.0 a 9.16.3,
- 9.11.14-S1 a 9.11.19-S1

El **CVE-2020-8618**, se da debido a un error de verificación de **assertion check** durante el procesamiento de grandes cantidades de **datos de archivos "zone".** Esta verificación es utilizada para prevenir que los datos de entrada vayan más allá del límite del buffer. Un atacante remoto que cuente con permisos para enviar **datos** de archivos **zone** al servidor, podría explotar exitosamente esta vulnerabilidad, causando una denegación de servicios (DoS) en clientes.

Por otro lado, el **CVE-2020-8619** se da durante el procesamiento del **carácter asterisco ("*")**en los archivos **DNS Zone**. Normalmente, dicho carácter se encuentra presente como una wildcard en un **nodo terminal** ubicado dentro del grafo **Domain Name System.** Sin embargo, BIND no válida que el carácter **asterisco** se encuentre solo en el nodo terminal. Esto podría generar un problema cuando un **asterisco** se encuentra presente en un **nodo vacío no**

terminal dentro del **grafo DNS**, en caso de que este nodo exista, luego de una serie de consultas podría llegar a un estado inconsistente resultando en un fallo de validación en el archivo **rbtdb.c**. Un atacante remoto con permisos para modificar contenido **zone** podría explotar esta vulnerabilidad causando una **Denegación de Servicio (DoS)**. Sin embargo,la explotación es poco probable ya que requiere un nivel significativo de privilegios y puede ser fácilmente rastreable.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante remoto con privilegios en el sistema causar una **Denegación de servicios (DoS**).

Solución y prevención:

Actualizar **ISC BIND** desde la **página web de descarga oficial,** a las siguientes versiones:

- **9.11.20,**
- **9.16.4 ,**
- **9.11.20-S1**

Información adicional:

- https://kb.isc.org/docs/cve-2020-8618
- https://kb.isc.org/docs/cve-2020-8619
- https://www.us-cert.gov/ncas/current-activity/2020/06/18/isc-releases-security-advisories-bind