CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: **10/10/2022**

Problemática: **Vulnerabilidad en los resolutores BIND (DNS UNIX)**

Correlativo: **AA-0037**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

Se ha emitió un comunicado para alertar sobre la vulnerabilidad identificada como CVE-2022-3080 que afecta a servidores DNS de sistemas UNIX en los resolutores BIND.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Bajo**	**Alto**	**Bajo**

SITUACIÓN

La información obtenida de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, detalla la falla en el paquete Bind, donde el resolutor puede fallar cuando la caché obsoleta y las respuestas obsoletas están habilitadas, la opción stale-answer-client-timeout está establecida en 0 y hay un CNAME obsoleto en la caché para una consulta entrante. Al enviar consultas específicas a la resolución, un atacante puede hacer que named se bloquee, y así afectar la disponibilidad de los sistemas.

Producto afectado:
Paquete Bind en las versiones 9.16.14 y posteriores, por lo tanto, Red Hat Enterprise Linux 6 y 7 no se ven afectados por esta vulnerabilidad

RECOMENDACIONES

- **El Centró Estratégico de Monitoreo-CEM recomienda a los usuarios del paquete resolutor Bind ejecutar el parche de seguridad emitido por el fabricante para mitigar la vulnerabilidad del software.**
- **Active las funciones de actualización automática de software en computadoras, teléfonos móviles y otros dispositivos conectados siempre que sea posible y pragmático.**
- **Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.**

REFERENCIAS

1. **https://access.redhat.com/security/cve/cve-2022-3080**
2. **https://bugzilla.redhat.com/show_bug.cgi?id=2128600**

DICCIONARIO DE DATOS

1. **Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo,**
2. **Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.**
3. **Parche de seguridad: Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.**
4. **Paquete Bind: Servidor de DNS especialmente en sistemas Unix, en los cuales es un estándar de facto.**
5. **Unix: Sistema operativo portable, multitarea y multiusuario.**

ÁREA PARA DEFINICIONES