CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: **10/10/2022**

Problemática: **Vulnerabilidad de Ruby-MySQL**

Correlativo: **AA-0036**

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

CONTEXTO

Se ha emitió un comunicado para alertar sobre la vulnerabilidad identificada como CVE-2022-38019 que afecta al conector MySQL para Ruby. La explotación de esta vulnerabilidad permite que un atacante remoto ejecute código arbitrario.

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**	**Bajo**	**Alto**

SITUACIÓN

La información obtenida de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, el conector MySQL para el lenguaje de programación Ruby presenta una vulnerabilidad, donde un servidor MySQL malicioso puede solicitar contenido de archivo local de un cliente que usa ruby-mysql sin la autorización explícita del usuario.

Producto afectado:
Ruby-mysql antes de la versión 2.10.0

RECOMENDACIONES

- **El Centró Estratégico de Monitoreo-CEM recomienda a los usuarios del conector Ruby-mysql 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38019**
2. **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38019**

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 (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto**
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.**

ÁREA PARA DEFINICIONES